"Forbidden" Reports

•Shoplifting techniques. •Free entry & drinks in bars & clubs. •Getting into theme parks for free. •Getting into concerts, games for free. •Getting into major sporting events for free. •Bootlegging concert tapes. •Pirating & doing the tapes. •Pirating concert videos. •Food for free. •ATM con jobs. •Physical methods on ATM's. •Electronic & computer scams on ATM's. •Bogus cards, using pin numbers on ATM's. •Knowing the tracks of an ATM. •Deposits at an ATM. •Misimplimentation of pin searchs on ATM's. •Hidden facts about credit cards. •Getting other peoples cards. •The credit card drop site. •How to build a bug detecter. •Bugging: where to get & how to use. •Mobile phone tracking equipment. •How to get free mail. •What is hacking? •How to use hacking to your advantage. •How to identify a computer & hack into. •Hacking conclusions. •Counterfeiting money. •Credit card fraud. •Picking master locks. •Lockpicking cars. •The art of lockpicking. •Highway radar jamming. •Easy way to hotwire cars. •Ripping off change machines. •Simple hacking. •Basics of hacking. •Hacking dec's. •Breaking into houses. •Jackpotting ATM's. •How to grow marijuana. •Growing marijuana outdoors. •General growing info. •Indoor growing. 2 page •Harvesting & drying. •Increasing the quality. •Trouble shooting suggestions. •Turning bad into good. •How to create a new identity. •Infinity transmitters for phone tapping. •LSD manufacture & dosage. •How to abuse a BBS. •What you should know about collection agencies. •Cash from other peoples credit cards. •Phone tapping. •Wiretapping, bugs on line etc. •How to make a simple listening devise. •How to make laughing gas. •Coin changer fraud. •Crimminals use teenage hackers. •Speed radar & defenses. •Opening safes using sound. •The science of opening safes. •Drilling safes. •Other methods to open safes. •Telephones & ATM fraud. •Microphones for surveilence. •Amplifiers & surveilence. •Signal types and processers. •Output simulators. •Chain lock picking. •Basic beginners lockpicking. •Picking combination locks. •How to crack a padlock. •How to crack dial locks. •Bypass lock techniques. •Door lock picking techniques. •Opening car doors. •Disc tumbler locks. •Practise makes perfect with lockpicking. •Lever tumbler locks. •Telephone phreak terminology. •Home made gun silencers. •Credit cards, security & fraud. •Alarms & finger prints. •Colour copying & anti fraud devises. •Post office fraud. •Making keys to enter machines. •Satellite T.V. cards. •Hacking into... •Sonic jammers. •Training & anti - terrorism schools. •Resources for above: goods & mags. •How to make a stun gun. •Computer dangers from hacking. •Fraud & public utilities. •The art of trashing. •Plastic explosives from bleech. •Solidox bombs. •CO2 explosives. •Touch explosives. •Letter bombs. •Paint bombs. •Smoke bombs. •Lighter ballistics. •Manufacturing explosives. •How to create a car smoke screen. •Car break ins. •House break ins. •Building a delay detonator. •Dealing with dynamite. •Making flash powder. •Making a carbide cannon. •The terrorist handbook. •Portable grenade launcher. •Home chemistry. •Blasting caps. •Meythal hydrate cannon. •Military explosives & uses. •Kitchen chemistry. •Napalm grenades. •Fire bombs. •Pocket rockets. •Counter intellegence challenges. •Espionage awareness. •Effective crowd control. •Custodial interrogation. •Brainwashing techniques. •Why suspects confess. •Cellular phone "free". •Scanner converters for cellular phones. •Cellular phone fraud. •Telephone charging box. •What to look for in a code hacking program. •Pay phones types. •Ethics & purpose of phone phreaking. •Detecting bugs on home phones. •The use of call diverters. •History of British phone phreaking. •Fax machine fun. •Fax interception & security. •Public fax machine fraud. •The gold phone box. •Phone dialing pad. •How to get money from payphones. •Basic phone evesdropping techniques. •Electronic toll fraud devises. •Illicit use of mobile phones. •Telephone fraud. •Money from payphones.

"What the hell is Bernsteining?" you well may ask. Well it's the term that my friends and I use to describe getting into places, getting things and doing things at no cost to us, but to others. Once you learn some basic techniques, it will be easy for you to become a hoarker of severe level. Hoarking is another term, which means basically the same thing. Several other terms have been used to describe the process, but these are the ones that I like. Hopefully I will be able to tell enough about Bernsteining to get you going, and I hope I make some sense.

There are several different ways of Bernsteining. One method is shoplifting. But not ordinary shoplifting, no no! I am not talking about shoving a package of ding dongs down your pants and sweating while sneaking out of the store. When you "hoarklift" you do it with style. Another Bernstein method is the one that I like the best, getting into places for free. This one covers almost the whole Bernstein spectrum. One that know the techniques can get into almost anyplace they desire for free, if not for considerably less than what it would cost an uninitiated Bernsteiner. The best thing about all this is it's fun as hell!   It's a great feeling to wake up in the morning with about $2.50 in change in your pocket, then by mid day be inside Walt Disney World, screwing with the old folks, eating your fill of junk in the Future World Cafe. Yes, it can be done, all for free if you know how. Hopefully, I can show you how, and the world can be full of Bernsteins.

****
Make for the shopping cart hoark...
****

Let's talk about hoarklifting. It's a lot like shoplifting in that you go into a store and walk out with something that you didn't pay for, and now own. If you were to go into a store, such as Skaggs, Albertsons, Publix, Winn Dixie, Jewel Osco, etc, etc, etc... you would not want to be shoving merchandise down your drawers. The boneheads that work at these stores are dumb, but not dumb enough to not notice large bulges in your pants. Also, you are very limited by what you can fit in your pants. Unless you are skinny and got yourself made up to be a heifer, there just ain't much room in there. The goal here is to get a LOT of stuff out of the store, and maybe even get some help taking it out to your car.

Ok, let's get down to the nitty gritty. Things you need... umm you need yourself of course, and you gotta be half way presentable. You gotta look like someone who would have a whole shopping cart of groceries. When selecting items to take, don't be stupid. Don't fill a cart with beer. Fill it with whatever most people get when they are at the store. You don't want to draw attention to yourself at all. You must look like an ordinary customer. So.., when you comb the aisles, with shopping list in hand, and fill your cart as you wish, start going up to the front. Ok, this step is when the talent comes in hand. Hopefully you are in a store with a large exit area, lots of aisles, and they all should be busy.. The best days are Saturdays, midday, on a cloudy or overcast day, when the most people are in the store. The aisles will be backed up, and all available employees will be running the registers. At this point you have to get out your receipt from another trip, or one that you find in the area. Scan the store before entering, looking for a nice long one, that is in good condition. If you got one in hand, proceed past the registers and to the front to the store. The busier the store, the more confused the employees will be. You may be spotted by a bag-person, and they will ask you if you want help taking the groceries to the car. If they ask this, gladly tell them yes, and have them push the cart out and into your car. Give em a tip, 50 cents or so. They will like that. If no clerks are around, go to the doors and exit. Make sure that you have the receipt in your hands. The reason this works is that the people who work at these places are usually only concerned with what is going on in their lane, and no where else. If it is really busy, then the front end management will be running around making voids and even running registers if it's busy enough. If a cashier sees you pushing your cart full of groceries around, with receipt in hand, they will assume that you have been checked out and are looking for help taking the cart out, or you are on your way out. Rarely will a cashier ask you what you are doing. They all assume that someone else did the checking on you, and you are leaving under good terms.

Okay, you've read the details, and I have made it sound fairly easy. That's because I have left the hard part out! If you noticed, the groceries haven't been bagged, which will look VERY suspicious if you try to push them out of the store. This is where the real skill comes in. In the process of filling your cart you have to bag the groceries. No one can see what you are doing. This becomes a real problem because this method is used at peak hours when the store fullest. One way I bag the groceries is to bunch up the bags at the bottom of the cart, so I can place the groceries on top of them, and when no one is looking, pull the sides of the bag up and around the groceries. You may be able to come up with your own methods for doing this. A simple way of bypassing the bagging is to get groceries that don't need to be put into bags, such as bottles, beer (suspicious), large boxes, etc. This all depends on what kind of layout the store has, and how full the store is. Another thing that may be of assistance to you is some stores have a "lobby" entrance at one side of the store. In these stores you may be able to avoid the front end all together, and push the cart around the magazine rack, or whatever the particular store may have, and out the side door. Whatever you decide to do, you can't be hesitant. You have to be utterly convinced that what you are doing is FOOLPROOF. If you have the slightest doubt in your mind that you will get snagged, don't do it! It isn't made to be executed by people without any balls (sorry if any girls are reading this, you obviously don't have any balls in the physical sense).

If you are questioned by someone in the store... well if you are stopped before you exit the front doors, act like you are looking for someone to ring you up. Act foreign, act retarded, just play STUPID! Don't ever admit or act like you know what you were really doing. Ask the person who is questioning you where you have to go to pay for your groceries.

If you are good, though, you can act like you paid for them and BS your way into the parking lot. But, if they ask to see your receipt, you are screwed. At this point, if they are about to get REALLY suspicious, then make a scene. Scream "why am I always treated like an idiot whenever I step into your shitty store! All I want to do is shop!", etc., etc... There is nothing worse to an employee than being yelled at by a customer in front of other employees and other customers. This will almost always get them to comply with what you want. If this works, stick with your story, and exit, or if you told them you would like to pay, have them show you where to get into line. If you exit, congratulations. If you end up in line, tuff luck. You gotta somehow get out of line and get the hell out of the store and don't try it again at that store. It might take you a couple times to get it down pat.

One thing that is important, if you haven't taken the groceries out of the door, and into the lot, you haven't stolen them! You can parade all day in front of the registers, and they can't do anything about it, because you haven't taken them out yet. So if you are stopped in front of the doors, before the exit, then you have done nothing wrong, and they can do nothing to you but ask you questions about if you have paid yet. Another good thing to say is "I was going to leave the cart here at the front while I ran out to my car for my wallet. I didn't want to leave the cart unattended in a line, because it would upset the other shoppers." This works well, it makes you sound like a real concerned shopper. If they say, "ok, we will watch it for you while you get your wallet" then go to get the wallet, and drive away. No luck that day. Just remember, as long as you are in the store you are safe, if you are followed outside and then asked if you have paid, then you are in deep shit. Hopefully you have enough brains to accomplish this task. In any case, I wish you luck, and lots of free groceries.

****
A tale of barage...
****

Ahhh... there's nothing like being able to get into a bar for free, especially if it's an exclusive club, and ESPECIALLY if you are under age. I am now of legal age, so I am left out by the ladder, but I started the bar hoarkin at a young age. Bars are very easy to get into for free. So easy, in fact, that my friends and I would often visit 4 or 5 different bars on a single Friday night without ever paying for anything but gas

One of the easiest methods of bar hoarking is the "tag" method. This is a way of getting in by using a "tag" given to people when they leave the bar so that they can get back in, bypassing any long lines. When you arrive at a bar, wait until you see people leaving the establishment, then observe what kind of tag they were given. It could be anything from a simple hand stamp, to a wrist band, to an elaborate ID card. Make sure you get all the details.

If the tag is a hand stamp, you are luck Hand stamps are very easy to forge. Most are single color, black, blue, or red. Maybe green or an off color, but nothing really unusual. Take note of the leaving person's stamp. Notice the size and placement. Be sure you know which hand is stamped. Most bars will only stamp a particular hand, so be careful you know which it is. Take note the "smearage" of the stamp. If the stamp on the person's hand is smudged a lot, that is good. If it is well defined, that means that the ink they are using dries and stays fast well. In this case a ball point pen is needed. You should be carrying a set of colored pens in the car, ball point and felt tip. After you got a good look at the person's stamp, try to re-create the stamp on your hand the best you can. If it is a box shape, try to make it the closest to the original size that you can. If the stamp on the person was smeared a lot, then use a felt tip pen. After you and your friends have drawn the stamps on yourselves, rub them lightly on a piece of cloth, so that they blur. No stamp given by a bar is perfect, and if they expect it to stay perfect while you are bumping up against people in the bar, they are crazy. If you think your stamps look good, then you are ready to enter the bar. When the bouncer checks for stamps, the light isn't usually good. They also usually have a different bouncer checking stamps than ID's, so then this bouncer might be more inside the club where there isn't as much light. Also, the fact that there is usually a line of people getting back in with stamps means that the bouncer will just glance at your hand, not really soaking up the details in the stamp. Most of the time that I have tried this, I have simply walked past the bouncer, and flagged the back of my hand with a "I gotta stamp...", and am returned with a grunt and a nod. Only once have I been turned down with this method, and that's because we were all laughing at the bouncer. (It was a gay bar with gay employees.) Once you are inside, you are home free. If you want to leave, make sure that you rub off the false stamp and get a real stamp as you leave, so you will be able to get back in for sure. Also, something good to do if you are at the bar very late, or if there just aren't too many people in the bar, and that is to try to steal the stamp. Most bars carry several of the same stamps, and the only difference between nights is that they change the color of the ink. My friends and I have a collection of 7 stamps from area clubs, all which work 100 percent. All we have to do is find out what color the ink is for that night and we are in.

Ok, enough with the stamps... what if the tag is wristbands. Well, that's simple. If you see someone leaving, ask for theirs. If they aren't planning on coming back that night, they will gladly give it to you. Keep a safety pin with you, because the bands usually tear when taken off. When you get a band, keep it. You can use it some other time. The bars and clubs do rotate bands, so after a while you will have several different colors. Many bars use these bands so they can be used in several different places. If there is a bar logo on the stamp, just make sure that if you use it in a different bar that you turn the band around so that the bouncer won't see the logo. Make sure you save these wristbands because they aren't only used by bars, but many other things, which I will talk about later.

Now..ID cards, some exclusive bars have ID cards, which are hard to duplicate. The best way to get one, is to steal one someone leaving the bar. Simple as that. Can you handle it? There are very few bars that use this method, so I don't think I need to get into detail. Just use your head.

Once in the bar... when you get in you wanna drink, and who wants to pay for drinks? A very simple thing to do is find a long stretch of bar table, in a dark section of the bar, and sit down, squeeze in, what ever you have to do. Try to position yourself next to someone who is really drunk. It is also good if people are far away from the bar towards the dance floor, or live band, whatever is going on at that particular bar.

Now, keep your eye on the bar. Watch for when someone sitting down orders a drink. It helps if the bar is really busy, because the bartenders will be running around like mad dogs with their dicks cut off. Most drunk people are so worried about drinking they order then slap their money down, then forget about the drink. If you have a chance, try to swipe the bill they lay on the table, or if it is more than one bill, take just half. Then when the bartender comes with the drinks they will ask the patron for the money. They should be drunk enough to think that they actually didn't put any money down, or didn't get enough money out of their pocket.

Ok, besides money to buy drinks, why not just take drinks? If the guy (or girl) you are seated next to is REALLY wasted, just slide their drink away from them when they first order it. Replace a rum and coke with just a coke, they shouldn't be able to tell the difference. If they order multiple drinks for friends and such, then take one. If you aren't scared of germs, take their drink after they've taken a sip. A lot of drunk people will drink a little bit of their drink then set it down and forget about it. If it is hard liquor you shouldn't be worried about germs, the alcohol should kill them. Beer, I am not too sure of, it doesn't contain too much alcohol as opposed to a vodka martini. It should be safe though, especially if they only took a sip from it. If you have a glass that you know is clean, reach over and dump half of their drink into your glass. Then they will feel proud that they could drink so fast, and order another drink. The drunker people get, the more the drinks will flow into one another, and soon they won't be sure of exactly what they ordered, and won't notice a missing cocktail here and there.

It sounds easy, it is easy. One important note, don't try this in a biker bar or one that you could easily get into a brawl in. A drink isn't worth your life. Another good way of getting free drinks works well in gay bars. You may not like the idea of going into a gay bar, but in my experience I haven't had a bad time in one. The gay people can tell if you are not gay, and leave you alone. Never have I been picked up on in a gay bar, and have even met a few girls in them (yes REAL girls, not prefab girls). The reason why these bars are good targets for free drinks is the fact that most of the gay people are in a good mood there, they are with people that they can get along with, and they don't like to cause, or be a part of any trouble. You can easily use this to your advantage. Order, steal, or somehow get your hands on a pitcher of beer, full, half full, or almost empty. Walk around with this pitcher. When you see a good target with his (her??) back to you, turn your back and bump into them, spilling anything that you had in the pitcher. If it wasn't much beer, act like it was full. Don't get mad or aggressive, just get sorrowful. Make them feel bad that they knocked the beer out of your hands. They should offer to buy you another, if not suggest to them that they should. Don't be too forceful, they will catch on if you are a dick to them. I have never encountered a homosexual that would not buy another pitcher of beer for me and my friends when this is used. When they do get you one, offer them a glass, be nice to them, they may buy you another. One important note, when in a gay bar, and a gay person seems to be making any kind of advance towards you or seems overly kind, just tell them that you aren't gay. They won't be offended, and they may even buy you a drink (our goal). They like to be treated like normal people, so if you are friendly to ones that kick your pitcher, they may be buying you pitchers all night long, as long as you are nice to them, and remember, all you have to do is tell them that you aren't gay. Well enough with the alternative lifestyles class haa...

****
Chilling toaster ovens and unidentified pizza rolls...
****

Alrighty kiddies, let's begin. Suppose you hit the weekend without a cent in your pocket. No worries. You know that you can do things that an ordinary person would not dare. If you have any kind of amusement park, or theme park where you live, it is very much possible to spend the day there without spending money, and without having to climb over a fence. All you need to do it is some intelligence, and a good knack for bullshitting. Try not to look too much like a scum ball. Look like a tourist.

If you are going to do it at Disney World, wear a Mickey Mouse shirt, etc. You have to realize that most all of the people who work at these places are teenagers and young people in general. They aren't too concerned of being really strict, just to stand in place and grab tickets from people filing by. Now, you have arrived at the park, and are at the front gate. What you must do is wait for a large group of tourist looking people to be going in. The larger, the better.

The best groups are ones with a lot of handicapped or mentally retarded people. In groups such as these, the tickets for the entire group are handled by one or two people. If you see something like this happening, go towards the entrance. As they start to go in, blend in with them. If only one of this group has the tickets, you are in luck. Try to act either really excited, or emotional about entering the park. If you are with retarded people, act a little slow, it isn't hard to do. Make sure you are in the middle of the group. Even the group shouldn't notice you until you are well inside, and by then you should be separated from them. If you want, put your arm around someone in the group as you pass through the gate. Say out loud "Isn't it great to go see Mickey!!!" Make sure that the person you have your arm around gets excited, but doesn't freak out. They should thing that you are just someone having a really good time. Sometimes they really enjoy this.

Now, you've been sitting around the park entrance for an hour, and no group has come. Well, there is usually a large line of people entering the park. If you see that the line is moving in a fairly fast stream, this is good. Get in line. When you get up to the ticket person, act retarted whatever you think will work and mutter to the employee, "he's (or she's) got my tickets," as you gesture behind you. By the time you squeeze through the gates and are inside far enough away, they will realize that there is one ticket missing from the whole deal, but most of the people who work at these places won't care. Sometimes when I have done this, the people in back of be have been refused entrance. I like when that happens. If you were lucky and got in this way, good. There isn't too much to worry about, as long as you weren't in sight when they discovered what was going on. If you put on a good mentally retarded act, you shouldn't be questioned.

Alright, what if there are no lines at all, or next to no lines. This is when bullshitting is your only tool to get in. Check out the people taking tickets. If it is slow they will be talking amongst themselves. Look for the person who is the "outcast" or not talking to the others. This may mean that they are shy, or new. Slowly walk to their line. If you have a hat, mash it down onto your head. When you get to them talk slowly and softly. Tell them that you were in the park with your mother and got lost. If you are older than a kid that would be with his mother, act retarded. Drool a bit. Tell them that you were with your mother and you got separated. You got really scared that she left, so you went out to the car, which was the only place that you knew how to get to for sure. When you got to the car you remembered her telling you before you went in that morning, "if we get separated meet me at the xxxxxx." Fill in with something that you know is in the park. If they ask you for a stub or something, act like you don't understand.

If they tell you that you can't go in without a ticket, start to cry. Stick to the story. If they get someone like a manager, stay with the story. Get more and more flustered and whiny the more they question you. Get them tears flowing!! It's good theatrics, and really fun to see how these react to you. Tell them all you want to do is get to the place your mother told you to meet her at and wait there for her. You might have an employee escort you to the spot. This has happened to me once, and that experience will be told about in Sportsage. If they find a person to escort you to the fictitious meeting place, seem relieved that you are there. Of course, your mother will be no where around. Tell them that you will have to wait there for her. After a few minutes of waiting they will either leave you alone there to wait, making you promise that you won't go anywhere, or they will ask you to leave. One thing, this method only works when you are alone. It would be hard to do this with more than 1 person. If they leave you alone, make sure they aren't going to be back in a while, then take off. You might want to wait until they come back to check up on you, that way they will really thing you are waiting for your mother. This method takes a long time to complete, but you feel really good when you successfully pull it off.

There are other ways like these that I have described, it's all up to your creative abilities.

Other notes... besides retarded people, you can grab onto old people too. They often come to theme parks in large groups, so they are a good target too! If you are stopped inside and accused of sneaking in, tell them you had a ticket and tell them to prove that you didn't. I don't think that there is a park that requires you to always carry a stub around proving that you paid to get in.

The only time I have been questioned at a park was when I used to hop the fence at Busch Gardens. If they see you enter like this they will most definitely go after you. Going in the front way is a lot better because the most they can make you do is get out of the way.

If you are stuck at the gate, and they are asking for a ticket, and you told them that the people you had it, and it gets fouled up somehow, act like the people you pointed to weren't the people that you meant. Say something like "holy cow, the people I were with are gone! They were right behind me!" This won't get you in, but it will keep you out of trouble. When this happens, leave the gate area and act pissed off that your friends left you, and try to get in later. It helps if there is more than one entrance. Also, if you are going with friends, go in separately. Unless you can squeeze in with a large group of tourists, it isn't advisable to be together. Have a meeting place arranged beforehand so that you can get back together once inside.

This all sounds real complicated, but it's almost too easy! As I said before, most of the people who work at these places are kids, and don't want to be bothered chasing after someone who squeezes through their line. So! Try this out and see what happens!

Taking the things I have talked about in hand, you adapt them towards other things, such as getting into concerts. There are a few things that are concert specific, though. A crowd at a concert is much different from one at an amusement park. It is a lot harder to sneak into a concert than a park, because there are not "tourist groups" to blend into. Also, you usually get frisked.

One method that has been used is fairly simple. You just have to get a ticket stub. If you can get one, get it. You may have to wait for someone leaving the show to give you their's. Or, if you know someone who has paid, have them hand you the stub through a gate, or some place that you can "intersect" around the place where the concert is held.

If you are more daring, try this method... go to the place of the show early in the day. Try to get around to where the equipment is being loaded into the arena, or whatever the place is. If you can, slip in and find a place to hide out until the show starts. This can be hard, and takes a lot of patience. Again, if you can, use the skills taught in the last chapter.

Another good ploy is the wheelchair method. A big show should have a separate handicapped entrance. Have a friend wheel you to it. Be covered with blankets, and have on a lot of the band's junk, like shirts, hats, etc, so that you look like a real fan. The best kind of handicapped person to be is one that can't talk, that just sits and does nothing..

Now, let me get something straight with you, I am not prejudiced against handicapped people, this is simply a method used to enter places for free. I am sure that anyone handicapped in this way who reads this will find it moderately amusing. Enough said.

Okay, you are at the handicapped entrance, and they ask for your tickets. You, of course, can't talk. Drool a little. If you had a friend bring you in, they should say something like "oh they are with the rest of the guys who are in another area." Have him ask the ticket takers to let you and your wheelchair sit inside so you won't get into any trouble. When he goes off, slowly wheel yourself to a good spot, and when they ticket takers aren't looking, slide in.

**   A Tale of the Super Bowl Hoark   **

****
Week of Boredom...
****

We had been doing nothing but bar hopping for weeks. We could get into any bar in the bay area for free now, so we took advantage of it and were out all night, every night. It was becoming quite dull. Another weekend was coming up. There wasn't much else to do but go to the bars again. We were planning on going into bars all weekend then watching the Super Bowl on television at whatever bar we would find ourselves at. That's right, it was Super Bowl Sunday heading our way. Now, I particularly don't care to watch football, or any sport for that matter, but the Super Bowl is something different. It's gigantic, it's stupendous, it's..it's... it's downright fucking big! It's the culmination of all the football season wrapped up into one game that would be exploited and smeared all over every television viewer's retina's across the entire world! Whew.. At some time during the week preceding this weekend of jock fantasy, it was suggested by one of us that we should drive down to Miami and sneak into the Super Bowl itself. We naturally agreed. I don't think that any of us really thought that we were gunna actually do it, but it made good conversation to talk about it. By the middle of the week we were talking about it more and more. At this time I realized that we were actually going to do it. I knew the bunch of us was crazy, but I didn't ever think that we would try something like that. Somehow we got our stuff together and made plans to leave for Miami on Friday night. Although I had a feeling we would have no problems, Wade and Drake were kind of doubtful that we could get in. It didn't matter to us, we knew that even if we couldn't get in we could have a fun time in Miami. Boy, was I juiced.

Friday came, and I got my stuff together for the trip. I was a bit over packed, I had a pair of jeans and a t-shirt in a plastic bag, a flask of rootbeer schnopps, and $20.00 cash. Miami is 6 hours away, and I figured the 20 bucks would just about cover my share of gas and any meals that we would have to pay for. The three of us all had something different to do on Friday evening. We planned on meeting at 2am and driving out to Miami. I had decided to spend my Friday night at a party. Wade and Drake were at a bar. By midnight I realized that I had gotten a little too drunk for the drive south. I left the party around 1, and got home around 1:30, and was pretty sloshed. I gathered my few items and double checked that I had all my crap. Making sure that I didn't have my toothbrush, I left the house. My destination was the end of my street, where Wade was to pick me up in his VW. Well, I sat and sat. It was 3am and he hadn't shown up yet. "He ain't coming, I better just go home and get to sleep," I thought, but as I did, the whining of his car ebbed from the darkness letting me know that he was on his way. Within seconds he was at my feet. The first thing I noticed was the drunken glow on his face, and Drake's. The reason he was late was because they had gotten held up at Drake's. I was supposed to be picked up first. No matter, we were on our way, all three of us drunk out of our minds, driving a too small too slow car towards a night of fog.

****

Enema Creeping

****

As the night went on we circulated the driving. My thinking grew hazy as I yearned for sleep. We were in the Everglades, on a stretch of road known as "Alligator Alley". None of us were in too good mental shape, and we were getting to the time when the alcohol was slowly wearing off, leaving us in a rotten sleepy mood. The past two hours were nothing but a haze of the 50 or so yards that was visible in the thickening fog. As the sun came up the visibility grew worse. I had no idea how much further it would be before we would see any sign of civilization besides litter on the sides of the road. Just about the point where I thought this to myself I noticed that we were just about to run out of gas. Drake had been driving at the time, Wade was sleeping in the back, and I had been up watching the road and making sure that Drake didn't fall asleep. I alerted Drake to the gas shortage, who in turn alerted Wade. Now it was panic time. Here we were in the middle of a gigantic swamp with almost no gas. The closer we came to running out, the farther anything was. We crept along at economy speed breathing with every chug of the motor. Every turn of the drive train was it's last. How many times can one hallucinate an engine stopping? It was driving me mad. All at once, we spotted some buildings. They crept up all around us. Huge, aluminium buildings with lots and lots of trucks parked next to them. Our hopes rose, we knew that we were close to gas! Smiles on our faces we drove... and drove... and drove. No gas. Fuck! Something was wrong! All these trucks, they have to use gas! Maybe they were left by some strange aliens that pioneered gasless trucks... nah. It was scary. We turned the first corner that we could. Tears welled in our sleep deprived stinging eyes. Then, as the car sputtered to it's last breath, we saw a station. Gleaming pumps, slick oil marks in giant welcoming circles across the pavement greeted us with a friendly feeling of warmth. We had made it to Miami.

****

Sunburnt spaghetti and flowering eyelids...

****

It wasn't long before we were past the gas station and in the heart of Miami. We all live in a shitty little county in Florida that consists of 80 percent old people and 19 percent hicks, leaving us and our friends wallowing in the left over 1. Miami was a mil iles away in difference. The traffic moved swiftly, and the cars were fast. It was a change from driving in a parade of Cadillacs going 10 miles per hour. The city sprawled around us, and we drove to Miami Beach. It was 9am when we got to the beach. After parking the car we decided to walk around and see the sights. When we first got onto the beach, we noticed that one of the larger hotels was sporting several limos. They were accompanied by a large "Welcome Bengals" banner. Ahh.. looks like one of the teams was here. That was where we were heading. When we reached the hotel we saw that the security was pretty tight. Lots of cops manned the doors. One thing that we know is that you can't get into any trouble for just walking into a place like this, so we did. We were inside in a second, and sitting at the lounge. I decided to call up a friend who lived in Miami. Since we had no place to stay the night, I thought that he may be able to help us out with a floor to sleep on. Finding a pay phone, I called him up. He was surprised to hear from me. We had gone to High School together, and now he was attending the University of Miami. He was glad to help us out with a place to sleep. Unfortunately, he was busy all day, playing his trumpet at various Super Bowl-related events across Miami all day and night. He informed me that his brother would be at the beach in a little bit to watch a volley ball tournament at Penrod's, and we should go meet him there. Well, I went and relayed the information to Drake and Wade, and we left the lounge (and a $20.00 drink bill)
.

Penrod's was just a short walk down the beach. We were all very fashed from the night's drinking and not sleeping, but we didn't want to waste a minute of time in Miami. The beach was huge. It blows the beach where we live away. Thousands of people were starting to file out onto the sand as the sun climbed higher into the midday sky. Penrods, if you don't know, is a large bar, with many individual bars across the country. one that we were at in Miami Beach is a big beach house looking building on the sand. There's a pool there, and several jacuzzis. The thing that interested us, though, was the BAR. It was a big 'un, all right. The more people that got onto the beach, the more people that lined up at the bar. This day there were several events going on. A large volleyball tournament was happening right out on the sand, while a jet ski race was working out in the water, and we were hoarking at the bar. Every time we could, we would steal someone's drink. We had become quite good at it, with all the bar hopping that we had been doing in the previous weeks. We drank and drank in the hot sun, looking for my friend's brother. We didn't see him. We decided to stroll around the beach. There was a booth with a Camel Cigarettes logo on it, and they were giving away some sort of dumb prize. After getting into line several times and playing the roulette-type game, we came up with 3 pairs of sunglasses, 10 plastic mugs, and 24 packs of Camel Cigarettes. Too bad none of us smoked. We took our new shit and walked down the beach. We were pretty drunk then, and started getting a little rowdy. As we walked through the ever-growing-more-crowded beach, we kicked sand on the dumb fuck looking people. The beers in our hands were quickly being emptied on girls' backs. A lot of people were getting pissed off, but who gives a shit. We took a pair of sunglasses and mangled them up. Then, we took turns going up to fat bikini-clad babes with these distorted glasses on, snot dripping out of our dork-looking noses, and made come-ons to them. It was fucking hilarious. We had never pissed off so many different people in such a short period of time. It was getting to be too much to take. The sun was growing hotter and hotter, and we weren't feeling to good. After waiting for hours for my friend's brother, we left and went to get some lunch. The lunch spot turned out to be Kentucky Fried Chicken. It was a very bad choice. Although we got some free food (by asking for the "complementary" fries, chicken, etc.. it works!) it sucked. Wade was getting sicker and sicker. We were all very sunburnt from the morning's activities, and still drunk. One thing that I should have known was not to drink in the hot sun. Wade should have remembered also. He was getting worse, so we drove to my friend's apartment where we thought that we could get some rest.

When we got to the apartment we saw that Dan, my friend's brother, had returned ome. He told us that he had been waiting at Penrods all afternoon and hadn't seen us. Oh well. We crashed there for a couple hours, and were planning on going to some bars that night, when Wade started throwing up. He was white as a baby's ass and puking like a vomit seive. The night looked bad. While Wade lay in bed moaning and drinking small amounts of water, me and Drake took off for downtown Miami. The buildings glimmered with giant projections of football players, players that we hoped that we would see in the next day's events. Enthusiasm ran through our blood as we sped down the freeways. Coconut Grove was our destination, where we knew that we could stir up some shit. We arrived there and were walking around, eyeing all the rich fucks in their Porche 959's. There were many a drink to hoark that evening, and we were full on poached dinners. I still had 18 dollars, as I only spent two so far on gas on the ride down. As the evening grew on, we became bored. It wasn't the same without all three of us fucking around like usual. We couldn't leave Wade alone with his head pounding and stomach surging. So, we packed up and left this hell hole, to go back and sleep and hopefully get into the Super Bowl the next morning.

Arriving back at the apartment, we saw that my friend was still out doing gigs with his trumpet. He wouldn't be back until 4 or 5 am. I didn't really feel like staying up to meet him that night, so we cooked some hoarked food and ate and went to sleep. In the morning I was awakened by someone tugging on my shoulder. It was Jim, my friend that I hadn't seen yet. "Hey Matt," he says to me, "I gotta play my horn down at some pre game show so I'll see ya around!" He left then, and that was all I saw of him the entire time we were in Miami. In a couple hours we were all awake, and groping around for beers. Wade was still feeling peckish, but his spirits were high becasue we were about to depart for Joe Robbie Stadium, where the Super Bowl was being played that afternoon.

We gathered up our few things and cleaned up any messes that we made in my friend's home, and were off. The Blue Beetle buzzed into the morning haze (or fog) and sped off towards our destination- The Super Bowl.

****

Holy Shit Batman!

****

When we got down to the stadium, we realized that it was a bit early. The parking lot was next to empty, with only stadium personel and entertainment people in it. That was good. The bad thing was that on the way to the stadium, reading a little pamphlet about the Super Bowl. It said that due to past years overcrowding of the parking lots, only those with tickets can get into the lot. Well that really sucked. How were we going to get into the game if we couldn't even get into the parking lot! It didn't bother us, though. We planned on telling the man at the parking lot gate that we were inside already, and had left to eat at Wendy's down the street, and that our tickets were locked up in a friend's car. We even spotted Jim's car parked inside, as he was in a band playing at a pre-game party. We did infact eat at Wendy's, so the story should have worked. We strolled up to the gate with Wendy's cups in our hands. This is when we got the yellows. Wade had been feeling sick still, and for some reason none of us was up to bullshitting the guard. We sat around the entrance for about an hour, when we gave the idea up. By then the guard had been watching us, and kind of knew what was up. I couldn't believe it! All the way down to Miami and we were chickening out! The sun grew hotter. We were in a vast cooking pot of asphalt, frying like a stuck flounder. Wade was about to drop. One thing that we did notice was that the people on the staff that were entering the gate had colored wristbands on, much like the ones given out at some local bars. There were large groups of staff people filing out of tour buses and going through the gate. Wade said "fuck it, I'm going in!" He tried to blend in with the employees, but he was a bit too obvoius, the only person without a tuxedo and bow tie. They told him to get the hell out. This really sucked. It looked like there was no way we could get in. We took a walk around and saw a million people with signs saying "I NEED TICKETS". Damn, so many people want to get into the game! How the hell were we going to do it? We had nothing better to do so we decided to fuck with the beggars. The first guy we approached, we told we had 3 tickets on the 20 yard line. He freaked. We told him that they were in our car, and to follow us. He offered $500.00 each for them, which we thought was really good. Turns out that most people scalping were getting $1000.00 to 1200.00 EACH for the damn things. Well, after about a mile of following us nowhere, he caught on and started screaming and hollering. I felt so bad that we had wasted this guy's time, when he could have been getting real tickets. Hah! We did it to a few more people, but Wade was still feeling sick. I came up with an idea, why not get someone with real tickets to drive us into the parking lot. This sounded good, so we went with it. We stood by the road, and any car that looked big enough for us to get into, we assaulted. A million people turned us down. This really sucked! We were doing this for close to an hour, when Wade almost collapsed. He had to sit down for a while, so we went to his car parked at the Wendy's and got in it. Wade and Drake were miserable. I was too. Someone suggested that we just go down to Penrod's and watch the game on their big screen television. "No way!" I exclaimed. I wasn't about to drive down to Miami to end up sitting in a god damn bar watching television! We HAD to get in now! We parked his car in a neighborhood where people were charging cars $20.00-$50.00 to park in their yards. Now, Wade had a small dent in the back side of his Bug, so when we parked and someone came out to ask us for money, we said "man, someone just threw a rock at the car! We need to get a cop!" Well, they agreed to let us park there so that we could go find a cop. This was a good sign, we were starting to get into the bullshitting mood.

Over a small hill we went, and came out on the outskirts of the parking lot. The cars were numerous, a slowing worm moving towards the entrance. Then, around the corner came a big camper. It had Ohio tags on it. It happens to be that Wade is from Ohio, so he knew that he could bullshit them. We waited until they were almost at the front of the stadium, and mad assault. Wade yelled "hey wassup! I am from Ohio too!" and from there it grew into a conversation of the various things in the state, to coming down to the Super Bowl. "Yea," Wade said, "we need a lift in!" By now they knew that we were friendly, so they opened the doors of the behemoth camper and let us in. I couldn't believe it, we were getting into the parking lot! The guys in the camper were cool, giving us beers and telling us how they have been to every Super Bowl since 1971. They paid their $50.00 dollar RV parking fee and rode up to the stadium. When they parked, we gave our thanks and took off into the crowd gathering around the entrance of the stadium. It was a festive mood spreading all around the elite 70,000 who had tickets to this game. We weren't planning on trying to get into the stadium for quite a while, as it was still pretty early in the morning. Over the past week we had been seeing commercials on MTV (ugh) for the big tailgate party they were supposed to be having in the parking lot of the Super Bowl. The Bangles were gunna be there, and all day they would broadcast from the lot. We planned on finding out where they were and fucking around with the goofball VJ's, but we couldn't find em. We were looking everywhere around where all the people were. There were a lot of tailgate parties going on, but no MTV. There was, however a large fenced off area with a small line of people going into it, so we decided to take a look. As we approached the line we saw a kid coming at us, apparently he had been turned away. He mumbled something about "invitation only" so we freaked. This seemed like something cool to do. The three of us got in line and planned to just cram ourselves through. The line was kind of thick, so we were packed in just right. When we got towards the front I noticed that we were the only people not holding little cards, invitations. I didn't worry though, the most that they could do is tell us to get out, which is what they did to me and Wade. Drake, however, somehow snuck by and got in. Me and Wade then went to another part of the area where the exit was. In a few minutes Drake came out and had a yellow wristband on his arm. The same kind of yellow wristband that Wade and I had in our pockets from a local bar! It was incredible! We put the bands on ourselves and went up to the entrance. When going through, we made sure that we didn't go by the guy that told us to get out before. It was only a matter of seconds before we were all inside the fenced off area. It was really strange. There were a lot of people milling about in tuxedos. Hmmm... it looked like we stumbled into something really important. Taking a look around we saw that there were big areas of food being passed out. Drake and Wade went to piss, so I went over to a table where some steaks were being cooked. I asked them how much a steak was, and they laughed. Wow, I couldn't believe it, they were free! This was too much! When Drake and Wade got back, I told them the news about the free food. Drake loved it, although Wade really didn't feel like eating. We heard a band start up in a tent nearby, so we went to check it out. Along the way over we picked up hot dogs, hamburgers, and bar-b-que ribs. Upon entering the tent, we noticed a long table against the back of the tent with a large amount people lined up along it. We knew instantly what it was.. A BAR!!! Free food was almost too good to handle, but this was the motherlode! All the free beer and cocktails we could handle! I was served up with 32oz Long Island Iced Teas, and Miller Genuine Draft longnecks, while Drake played Russian Roulette with whatever the bartender would slap together. We drank a few, then refilled to take a look around. So far we had blown away any hoarking we had done, and we hadn't even gotten into the stadium yet. As we walked around, I noticed that there were quite a few "stars" in the crowd. We saw Don Johnson, Chevy Chase, etc... Wade pointed out some famous football players. When we had gotten over to the other side of the area, we noticed two trucks surrounded by television cameras. It was MTV! The first thing that came to my mind was what kind of assholes these people were telling people for weeks about a big parking lot party, when actually they were in a private area performing for a bunch of rich people's kids. On one truck was Ken Ober(?), the dickhead from Remote Control. Kevin Seals was on another truck with the guy that plays the whale Rozanne Barr's TV husband. The few teenage, and young people, that were in the area were all around the cars. On TV it looked pretty packed, but in reality there weren't too many people in there. The trucks were parked close to a fence, and on the other side of the fence were thousands of screaming kids dying to get into the place where we were. What a pitiful sight. There we were, without even a ticket to get into the parking lot, inside an exclusive party. We heard a cameraman counting down, then on zero they suddenly went live. The dicks sprung into action, sucking up to America, and they had a contest with some rich kids plucking rubber alligators out of gatorade coolers with their mouths. What a sight. Randy the hippie guy was there, he was such a loser. It was really funny watching how these people operated, how they made everything seem so exciting. Between live shots the small crowd was being "coached" on how to scream and shout, after all, they were going to be on MTV! (god) We went and got another drink then came back. When we got back to the trucks, we saw that the Bangles were there. I thought they would be cool, you know, but they were really strange. It was like the were on downers or something. We asked them if we could get up onto the truck with them, and one of them said "sure dudes", so up we went. Ken Ober(?) was up there with them with a bottle of champagne. It was 6 seconds to live time, and we were right up there with them. When they went live, the Bangles changed from down to hyper. They were saying shit like "this is the grooviest party we've ever been to!" It was sickening. Ken Ober (is that the fucker's name, or is it Kent?) was chugging the champagne and was about as drunk as we were. While live we stood with them all and I made strange gestures at the camera while Wade just looked like one of the group. Drake, however, stood right behind Ober, and screamed, "you're a DICK!!!" over and over. Now, this is all hard to believe, I know. However, before we left to Miami I told a friend to leave his VCR taping MTV all day Sunday, as I knew that somehow we would get on. So.. I have the tape of us doing all this. It's our only actual proof that we were in there, and I think it's good enough proof. In the video you can barely hear Drake screaming at Ober that he's a dick, and I look like the normal fool I am, and Wade looks like he's just hanging out with the Bangles. It was really neat. The MTV idiots finished what they were doing and when "Cut!" was heard, they reverted into their original boring selves. The Bangles were friendly, and autographed a nerf football that we stole out of one of the trucks. One of them had a "No Acid" shirt, hmmmm I thought they were a psychedelic type of band. Strangeness permeated the air around those bright haired babes, so we split their "groovin" scene.

Walking around the place we saw some more famous people. We kept eating all the food we could eat, and drinking all that we could carry with one trip to the bar. There were all kinds of stran displays in the area, the place was made up to look like Florida swamp land or something. There was a Seminole Indian wrestling an alligator, who had it's schnozz wrapped up with cable. It was a pitiful display, although I could tell that the foreigners thought it was spectacular. One of the displays happened to be a booth, with some scantily-clad gals behind it. We went up and asked them what the hell the booth was for, and they handed us all Super Bowl caps. They were pretty nice, with flower patterns across the back. They weren't like the cheap ones that the vendors were selling to the throngs of "normal" (heh) people outside the party. Wearing these hats designated us as one of the elite few with the privilege to get into this shithole of snobs. We asked one of the girls exactly what orginazation was holding this party, and they told us that it was being thrown by the NFL Association. That explained a lot. Well, we were pretty mellowed out, but still nervous about what we had to do next, sneak through the gate of the stadium. A few more drinks and we decided to leave the party for a few minutes and look around the entrances to the stadium to see which would be the best to try to Bernstein our way through. We all made sure to get new wristbands when leaving the fenced off area. The parking lot was now much more full. A lot of the crowd was trying to look over the fence and into the party that we were just in. A couple people asked us how to get into it, and we told them "gotta be invited, you loser." It was cool. Well, we had to look for a way in now, so off we went...

****

Loneliness at the Gate...

****

Our intent was to scan the gates, and see which would look like the best to cram through. When we walked out of the place a black man came up to us and asked us what the party was for. We told him it was the NFL association and you could get in with a wristband. Drake then sold one of the bands he had to the guy for 5 bucks, and it didn't fit around his wrist! The guy was just looking for some fun. It was still kind of early and only probally half of the crowd was there yet. We started to walk around the stadium in a big circle. I noticed that the other side of it had no cars parked in the lot yet. Apparently, they were filling up the parking lot in a certain order, and it had not yet gotten full enough to reach the other side. As we swung around the the opposite of the crowd side, Drake noticed that even though there were no people on this side, there were open gates. In one of them stood 3 hispanic looking women, waiting for someone to go in that side of the stadium. Well, I thought we were just going to look the place over, and so did Wade, so it was very unexpected when Drake shot ahead of us and slid right through the gate!! He just held up the yellow wrist band and walked through. Now this left me and Wade freaking! The lady he went by was confused, to say the least. Wade said "come on!" and went up to her. A security guard came out of no where and we shit our pants when he told Wade he couldn't go in... with the nerf football. He gladly surrendered it and went in, and I followed, with my wristband held high. I heard the security guard saying something like "fuckin' press assholes..." Jesus I couldn't believe it, we were IN THE STADIUM!!! Our goal had been accomplished! We sped up to the top of the place to get a good look at our surroundings. Only a few thousand people had entered the stadium yet, it was still 2 hours till kickoff. We found a payphone and Wade called his girlfriend back where we live. She couldn't believe that we were really inside the stadium. I tried callin my ma, but the long distance lines were all busy. We went to the food boots and filled up our cups with draft beer when the servants weren't looking. It was a spectacular sight when we entered the "bowl" of the stadium. The crowd was starting to fill the seats, and it was a clear blue day. Earlier that morning it had rained, so we thought that we might not want to go in if it was raining. But it had cleared up and now everything seemed perfect. We sat in some untaken seats and sat to wait until someone came along and told us we were in their seats. We noticed that on each seat was a nice seat cushion, and each was either red, blue, or white. On one side it said something to the effect of "hold these above your head at the half time show when prompted to do so and be part of the biggest magic trick in history." Well, this meant a good oppertunity to fuck around, so we scrambled up a bunch of them wherever we could. I didn't ever see how they turned out at the half time show, but I am sure it didn't come out as they planned! We grabbed some cushions to take home with us and moved into different seats. After almost a half an hour some people came and told us we were in their seats... so we moved to some others, and kept bouncing around. The bouncings became more frequent as the stadium became more and more filled. It was at this time that we realized that we wouldn't be able to find three seats together. We decided to split up. The game was to start in thirty minutes, so the stadium was just about filled. By this time there were no seats barely at all for us to sit in. We split up like planned, with arrangements to meet outside at the party entrance after the game had ended, or after we got kicked out, whichever came first. Well, I went up to the top of the 40 yard line stairs..where I stood up against the wall. I was thinking that I had a pretty boring few hours ahead of me. I didn't really care for football too much, and now that I was alone I didn't have anyone to mess around with.

I was standing there watching Billy Joel sing the National

Anthem. Wow.. I couldn't believe that I was in this place. Thousands of people were in all directions, all who had payed up to $2000.00 a fucking seat! It felt so good knowing that I didn't pay a cent. Well the pre-game show started, and I was getting bored. I couldn't bear sitting up against this wall an entire game, even if it was the Super Bowl. About the same time I realized this, I looked over to the next aisle, to see if I could spot where Drake or Wade was. Well they weren't there, but there were some security dicks checking the people standing up at the next aisle for their ticket stubs. Shit! I knew that they would come up my lane soon, so I decided to split. All the fun shit was over, like the jets flying over and the fireworks, all that was left till half time was some goofballs tossing around a dead pig. I took off then, down the steps, not knowing really what I was going to do.

****
Electronic Derby and L.L. Special k...
****

I wandered around the people for a while, acting like I was looking for my seat. This gave me a chance to knock the beers and cokes out of the idiot's hands. They loved me for it. I found my way to the outside rim of the stadium, to get a look at the lot. I saw all the help people in tents in the lot having to watch the game on lots of televisions. That must have sucked for them to work for the damn place and not be able to get in! I walked down the spiral embankment that ran along the sides of the bowl. Upon getting to the middle section I noticed a series of glass doors with large letters saying something like "suite 32a-46b". Wow, it looked like the VIP boxes. I stood around a corner and watched for a while at the people going into the doors. They would each approach the girls at the doors, and show their stubs and get in. Hmmm... I wanted to get in there bad, so I thought up a plan. I went to another entrance, as the one that I had first seen I had sat by for a long time, so I looked suspicious. Before going around the corner to the next entrance I smashed my cap down on my head, and tucked my hair up into it. As I walked around the spiral towards the doors I looked like I was retarded. I sat on the rail looking over the parking lot and acted like I was sick or something, taking in deep breaths of air. The girls at the door were watching me for sure, they had to be, I was the only one around. While I was getting "sick" I looked above the doors at the numbers listed. I picked out 34b as one of the ones in the sequence. After a few minutes of standing at the railing looking bewildered and sick, I stumbled over to the doors. The first thing I said was "is 34b heeere?" and drooled a little. The girl was obviously having a hard time dealing with the situation, she was very uncomfortable with the idea of a "special" person asking her a question, which is sad. But, at this moment, it was in my advantage.

She said "yes, 34b is here, let me see your ticket stub..."
"Huh?" I acted as though I didn't know what a ticket stub was.
"I need to see your stub, the leftover of your ticket."

I acted really confused about it, then I said "I was inside and I got sick and my mother told me to go and get fresh air and th
d I breathed air and I looked to go back in and I got lost

and I found a guy and he said this was it I need to get back in!" Panic rose in my voice as I sprawled words out to her. Tears started to well in my drooping eyes. "I can't let you in without a ticket stub, I'm sorry!" she said, but still held the door open as if she wanted to let me in. Obviously she didn't have the authority, or was afraid to get into trouble if she would let me in. "My mother is worrying about me she will be mad. I hate it when she gets mad oh no..!!" I rambled on and my tears grew thicker along with the bullshit. She was showing more and more pity as I cried.

"Well, let me get my supervisor..." She closed the doors and went out of sight for a moment, then came back with another girl who looked about the same "rank". She told the story to her "supervisor" that I told her. They thought I couldn't hear, and I heard them talking about the wristband I had on, and how only people who were in the NFL assocition had them, also my hat seemed special, because they were only given out to a few people. I went over to them then and said, with tears streaming, "I gotta get to see my mother she just gave me this to go out!" I showed them my wristband as I said this, so they thought that I had the band to designate myself as "special" so that I could get back in. Well, the "supervisor" girl told me that she would escort me to 34b and help me locate my mother. I freaked that I would get in, but not at the fact that this person would be along for the ride!

****

Pasta Fishsticks and Scary Furry Toes...

****

Well, I headed into the "elite" section of the stadium, along side a girl with an emblazoned SECURITY on her jacket. She had her arm around me to calm me down, as I was hyperventilating (heh heh). We walked down a corridor and came to some doors, each marked 34b. One was a private room, while the other was a pair of down into some stands. She asked me which my mother was in and I shit. Which should I pick? I started to breathe real heavy and hard and stuttered "I...don't..re..member...which...I...was..in..!!!" She tried to calm me down and asked me some simple questions about what the place looked like that I was in. I decided to tell her it was outside since the probability of me conning anyone into acting like my parents in that small room was next to finding no cancer in Ronald Reagan's asshole. When I told her that, she led me down the stairs and into some stands.

The stands consisted of about 15 rows of seats, if you have ever seen pictures of the stadium, or have been there, it's the small ring of seats in the middle, between the lower and top decks. We went to the bottom of the steps and looked up, so that we had a good view of all that was there. She then asked me if I saw my mother. Of corse I told her no. She then asked me if I was sure it was 34b. I told her "I think so...duh" as I began to cry again. While she was running down the list of bullshit questions to me, I noticed that about 5 rows up was a group of 4 seats together that was vacant. I turned away from her and looked at the game. This made it look like I wasn't paying attention to the empty seats. I "reenacted" the scene for her. I looked out over the field and said "Ok, I was here I know it I remember that helmet (There was a big helmet that they blasted balloons out of before the game in the corner where we were) and it was me, my mom, my dad, and my brother together then I got sick and went to get air because a man was smoking."

She looked behind us to the area that contained the four empty seats. When she spotted them, she whirled me around and said "Is that where you were?" while pointing to them. "Yes!! We were right there but my mom isn't there now! She must be looking for me!"

"Well, I suppose she is, I better take you where she could find you easily." She escorted me back up the steps and into the hall. Across the hall was a lounge, and some sofas. She sat me down on one. "Now listen, I can't stay with you all day. Your mother and father are apparently looking for you, so sit here and keep an eye out for them! I will come back in a few minutes to check on you."

"Ok I will!" I said with feigned glee. She walked off leaving me alone on this sofa. I knew I would have to wait a while before I was safely alone and could walk around. I sat and looked around. There was a bar next to me, and several televisions above my head. They were on the game. I was watching the television when the girl came back.

"Hey turn around and watch the hallway so you can spot your mother! Don't watch the television if you need to find your parents!"

"I'm sorry I forgot" I said with a pitiful look in my eyes.

"Ok, now I think you can be alright if you need anything just find someone in a yellow jacket like this one and ask for help, ok?"

"Yea, thank you very much you have been good help for me!"

"Alright she walked off. I knew that I could escape now, but I didn't want to be on this level with all the people that have already seen me around. I spotted a spiral staircase next to the bar, leading up. I knew that was my destination.

When I knew that no security was eyeballing me, I headed up the steps. When I got to the top I saw that it looked a lot like the bottom level, except that there were only private rooms, and no outside seats. I traveled along the hall, in a big circle all around the stadium. There were doors on the field side all the way around it. I spotted a door that was open, and putting on my retarded act, peeked in. It was full of business men drinking and eating while watching the game through a large plate of glass. They were all sitting on comfortable sofas, and there was a hibachi going with some food being cooked on it. There was a television in the corner, too, tuned into the game. Now this was first class! One of the guys spotted me, he was very drunk. "Look what we got here, the American skateboard champ!" He blasted his words loudly across the room. Now, I don't think I look like a skater, but this guy thought I did, I guess. When he yell out in this way, all the goofs in the room turned around at me. I smiled and kept watching the game through their room. After a while one of the guys got up and told me to leave. I guess I did kinda stand out.. I was the only one not dressed up.

Walking around some more, I watched the waiters delivering food to the rooms, lts of food on big rolling carts. This place was unbelievable. I followed the cart around and looked into the rooms that it entered, to see who was in them. I saw all sorts of stars and shit, from Don Johnson on.. a lot of the same people who were in the Pre-Game party. I got bored of walking around, and I couldn't really see the fucking game, so I sat up against a pillar and looked into a room which had an open door, and was about 5 feet in front of me. Right next to the open door was the press box, at least that's what the door said on it. There would be a person going in or going out every few minutes, and each time the door opened, I could hear the commotion coming out. I was standing there bored, trying to get a glimpse of the game through the cracks between the people in the room in front of me, when Tommy Lasorda came out of the press box and went into the room. He wandered around in there, and then everyone got up and started to come out. I figured out that it was half time. Tommy Lasorda came out again, and he was with OJ Simpson. This was pretty cool. They stood around bullshitting about the game and crap like that. This was the point that I wished that I brought a camera, because I knew that everyone, even Wade and Drake wouldn't believe this shit! Some television crews came out of no where and were interviewing OJ and some other guy. They were asking the guy about what it sounded like allegations of something and he was kicked out of the season or some crap. He got pissed off when they asked him about it.

There were many people I recognized walking around then. I don't keep up too much on the stars, but I could tell their by their faces that I had seen them before. I walked around some, and found a room that I could view the tv to see the half time show. It sucked. That's all there is to it, it was terrible. No one was paying attention to it anyways. This place was so weird. Everyone was dressed up like they were going to a formal event or something. I was wearing a dyed shit and a ripped up vest. (I don't think I fit in too well...) The show was about over, and the idiots started filing back into their cells. I went back to the pillar and leaned up against it. The room there hadn't had it's door closed all night, so I could kinda act like I was part of the group in there.

I was standing there a while when I felt a tap on my shoulder. I looked over to see a girl in a yellow SECURITY jacket. My heart shuddered. I knew this wouldn't last long.

"Are you watching the game in that room?" she asks.

"Well, kinda... not really, I'm waiting for a friend who's in the bathroom, I was just standing here so I wouldn't miss anything."

"Darn, well then you wouldn't know if that's Huey Lewis would you? I'd die for his autograph!"

Christ, I almost shit my pants! All she wanted was Huey's signature. "I don't know if that's him, I haven't really looked good." We stood there for a while, then the guy she thought was Huey Lewis stood up to get a drink. Sure was him. She got up the courage and went in and got his autograph. When she came back she was beaming. I was glad that she wasn't busting me. It was too damn close! It was extremely bored and kept walking around...walking around..in circles around the entire stadium. I must have done 500 laps that night. I thought about that I had probally done the same distance as any of the players in the game. I stopped for a while by a balcony and leaned up against it. There was a closed door facing me across the hall. As I was standing there, two men stepped out of it and stood on either side of the door. I didn't really notice them, except they were the only ones in the hall then. I still had my seat cushion with me, and for some reason (fidgeting probally) I balled it up around my hand. So I looked like this.. a bum standing there with a cushion under his right arm, with his left hand tucked into it. Well, the men across the hall must have thought I looked strange, because one of them started to stare at me. Then he motioned to the other to look at me. I acted like I didn't notice them, but I could tell they were worried. They must have thought I had a gun! I decided to play some games with them. The cushion had a zipper running down the edge of it, so I pulled my left hand out of the cushion, and slowly unzipped it. Then, I very slowly put it in the cushion. They were stiffening up quite a bit. One of them unbuttoned his jacket and I could see the butt of a gun poking out of his belt. Man!

Who were these guys. I knew they had to protecting someone in that fucking room. My hand was still in the cushion, I was acting like I was digging around for something in it, then WHAM I pulled it out real fast! Those guys almost jumped through the ceiling! Of corse, I had nothing in my hand... Well, I kept on fucking with them, I would put my hand into my inside vest pocket (a good place for a gun heh heh) and pull out a package of crackers or something. Each time, they would jump. I knew that they wouldn't let up watching me, they probally thought I was doing a purposeful "cry wolf" technique, and if they were any real security they should know better than to ignore me. Then, I unzipped the cushion again, reached my hand into it, fiddled around, then zipped it back up. All done very slowly. I then bent over and set it down on the ground next to an ash tray and walked off. When I got down the hall I turned around, and saw that one of the fuckers was already at the ashtray, stomping out a cigarette that he had just lit. He gave the cushion a little tap with his foot (not too smart if it were a bomb). I walked back when he was still by it and picked it up. "Oops! I seem to have dropped my seat cushion!" I said it with so much Disney glee that I could see the vomit rising in his gut.

Well I guess they thought less of me as a threat now, because they weren't watching me too closely. The security girl that had been hot for Huey Lewis walked by and I stopped her. "Who is in there?" I asked.

"I don't know, they won't let anyone in, not even us!"

"Wow, I gotta see this dickhead!"

"Yea, let me know who it was!"

"Deal!" She walked off and I waited. It was fourth quarter and the game was dragging on. I had no idea what the score was. I could hear the crowd cheering and moaning outside, and various yelps from the rooms. It was hell. After a few minutes, maybe an hour, a guy poked his head out of the secret door and yelled to the two guards. They had walked away from their "pet a drink. They were informed that "he wants to leave now!"

Wow..looked like a real event was about to happen. I made sure to get close to the door. I was directly across from it, leaning against the balcony, when it opened. The two men had their jackets unbuttoned so that you could see badges on their belts. Their guns were promenent features of their wardrobe. They started walking, then out of the door came more guards, and more. They were having a little parade, it looked like. Who the fuck were they guarding? Then, my question was answered, it was none other than Jimmy Carter (hah!). When he came out I yanked my hand out of my cushion to wave. The guards didn't like it too much but Jimmy didn't care, he waved back. I screamed "Luv ya Jimmy!" and laughed. There wasn't anyone else in the hall and here I was screaming at the top of my lungs at an ex-president of the United States. He smiled at me and nodded. He looked really fucking old. I'd hate to see Ronald Reagan up close in real life, he's probally like walking death if

Carter looked that bad! Well..the guards figured out that I wasn't a threat, and kept on marching away. They went around the corner and were gone. Well, so much for my "brush with fame".

****

Toadstools abounding!

****

Well, I was really fucking sick and tired of this place. I thought about leaving, or going somewhere else. I t to get into the press box, but they wouldn't let anyone in there without a special pass, and I didn't think I could bullshit a place like that, or want to. I was through with bullshitting for the night. I walked over to the elevators and contemplated leaving. There were only a few minutes left in the game. As I was standing there, some people came over to me. One was a security guard. She asked why I was missing the game standing around. I told her that my dad was a photographer and got me in on a press pass, but I don't have any "official" seats. Well, she didn't like the sound of that. She asked me where my pass was and I showed her my wristband.

"Hmmm...well let's go talk to my supervisor, no one said anything about this to me. No one is supposed to be on this level without a special pass" she said.

"Well I was going to leave anyways" I said, and jumped into an open elevator. Oh well, I had gotten through most of the game without being caught, and I thought about how the hell tdn't notice me standing around before! The elevator got to the bottom (it went all the way to ground level) and I got out. I walked straight out into the parking lot.

I had done it. Gotten into the game and even a little further than I had expected. I sat around in the parking lot and watched the people who hadn't gotten into the game wander around. I guess they must have gotten at least into the lot. What an accomplishment! Heh heh! There was a little commotion when two guys tried to scale fence and got the shit beat out of them by security guards. I wandered over to the tent where the pre-game party was. It was as desolate as a whale's ass. There was another tent nearby with a party starting up in it. Apparently it was for the employees. I showed them my band and wandered in, and it sucked. I left and went to the spot where I was supposed to meet Wade and Drake, back in front of the party tent. I could hear the crowd roaring in the stadium along with a radio broadcast that someone was blaring nearby. The taxicabs were lining up on one side of the stadium, and the limos on the other. The game ended suddenly, and there was a rush of people cascading out of the entrances. The first ones were running, probally to get out of the parking lot. They flowed and flowed, all with seat cushions in hand. I squeezed mine against my chest, to make sure I REALLY had one. I still couldn't fathom what we had done. Sure, we had gotten into Disney, Epcot, and places like that, and bars-a-plenty, but nothing, NOTHING like this. I wanted to cry (hee hee). I watched the crowd for a long time, then finally spotted Wade and Drake. The smiles on their faces were as big as the crowd. We met up and started telling each other our experiences. Wade and Drake found some seats and watched the whole game. They talked about throwing ice on people and ripping off shit from people, etc. I told them my story and they were surprised that I pulled it off. Well, what did they expect, I didn't really want to watch the game, and I didn't want to sit around all night. Well, we walked about a mile back to the car, and fortunately it was in one piece. After barely making it out of some sugar sand, we were on our way home.

****

Concludinado...

****

The weekend was great, I will always remember it, and now that I have it written down I won't forget all the details ten years from now. It all went without a hitch... except for this, on the ride home I got a speeding ticket right in themiddle of Alligator Alley! It was fucking 3am and the road is like 250miles long of just a straight road! Well, even the radar dector didn't help, we were the only ones on the road, and I happened to be the driver of the bug. Wade and Drake were asleep, and the pig waited until I was within 100 yards before he turned the gun on. The dectector lit up like the fourth of July! There was no way I'd get out of it, he followed me for a while then pulled me over and slapped me with a $128.00 fine. I was clocked at only 71, the bug is a slowmobile, but they are really worried about someone slamming into a panther at night, coz there's only like 12 left in the Everglades. Oh well, I paid if off last week, only 3 months late. So I guess the weekend wasn't ENTIRELY cheap.

****

Ol!

****

Your favorite band is coming to town and you got great tickets. You haven't seen them in years, and it's probally the last time they will tour. You manage to sneak in your walkman recorder into the concert hoping to preserve these moments in history. When it's all over you can't wait to hear how it all came out. You run to the parking lot and pop the tape in your car deck. You rewind it with fury, you can't fucking wait! You stop it in the middle to see how it sounds. Hmmm..this can't be right, it's like listening to bugs in a tin can! Somehow the whole thing got fucked up. It must be the deck, you think to yourself. Well, it's too late now to do anything about it, you made a two hour recording of large reverberations and crowd noise.

So, what can you do to get a good tape out of a concert? The concepts are fairly simple. It all depends on several things, though, but once you are familiar with them you can achieve high-fidelity recordings even if the hall is an echo pit.

****
Huh?
****

Okay. First thing that you need is a GOOD deck. Not something you bought at a flea market that has a little slit in it labeled "MIC". You need something that AT LEAST records in stereo. That's (if you didn't know) where you are recording two channels at once. You can pay anywhere from $50.00 to $500.00 for one of these. The price usually depends on the brand name and the size of the deck. Also it depends on the features. If you have the money to get a nice one (or some other method of getting one), get it. It will do much better in the long run. When looking for a deck you will want to look for these things:

* 2 Microphone Jacks, labeled L and R, or a jack that has a stereo adapter to be used with L and R microphones.
* Dolby of some sort. I like to use Dolby C. Dolby B is good also, but any will help.
* Variable level controls. This is so you can adjust the input levels. Decks with automatic levels record all one volume, and then when the sound drops out, the levels rise, also you get a drop out when a loud sound is made, knocking the levels down until they can raise back up to a desired level.
* Speed control. This is good for tuning the tape, or changing speeds. Also, you can maybe get a better frequency response if you run the tape at the fastest speed, but then you have to use the same deck to make copied of the tape.
* A radio on the deck. This is because if you get stopped with it at the door and they ask what it is just say "a radio" and tune it in. I have told them that a couple times when caught, and they say "I guess radios are allowed, just not tape decks". (Yea most of them are dumb asses) This works good with the very small tape decks.

Alright, if you get a deck with these things you should be set. The levels aren't that important, only if you are striving for a really good tape to maybe commercialize. You do have to remember that some places confiscate decks if they catch you sneaking one in, so be ready to lose it. If you can't afford a real expensive one, a cheaper one will do until you get used to sneaking them into shows.

Microphones. You gotta get some good ones, not little tape recorder ones that you get with those voice recorders, but ones made for music recording. I have used some Radio Shack mic's, the ones that look like magic markers, only longer. They are very thin. They require one AA (I think, the real small ones) battery each, and have a long cord. You need to get two of them, to use the stereo sound option. If you have a deck with just one plug, you need to make an adapter that will let you plug the two mic's in and get stereo sound. This isn't hard to do, you can even buy a cable for it from Radio Shack for like 5 bucks. Oh, the mic's are like 19.95 each. What is good about the microphones is that they are small and can be fit into your shoes upon entering a show. I have also used the "2 headed" stereo microphone from Radio Shack. It works okay, but is kind of awkward to sneak in. When you have the deck and the mic's you are set, all you need to do is get the supplies, tapes and batteries.

Tapes make a big difference in the sound quality of the recording. Don't use a cheap tape. A good tape can make you some bucks, so don't get something that won't sound good. I always use Denon metal tapes, 60 minutes. Longer tapes can get eaten easily in a walkman type deck, and since most people at a show will be moving around a bit, you will be most likely shaking the deck a little. This improves the chances of getting the tape sucked up. A 60 minute is a good size without the same chances of getting eaten. Batteries are easy to get too.. I'm sure you know which are good, get some good alkaline ones, and make sure that you are carrying a couple sets. It's not a waste to have too many batteries, you can always use them next time.

****

I'm Losing my Mind!

****

It's the day of the show and you need to plan your entrance. If you live up north, chances are that it will be cold. Then you can wear a heavy jacket. This is where a small deck will be good. I have used heavy jackets to put the deck in the lining in the back of it, with padding all around the deck, so when they pat you down they won't feel it. I don't think I have ever been caught doing it that way. If you don't have a jacket like that, or it's too hot, like it always is here in Florida, you gotta find another place for the deck. Something you can do is go to the show and watch people going in before you decide where to put the deck. Check out the security and watch where they are patting the people down, then put the deck where they aren't feeling. Sometimes they avoid the lower leg, then you can put it in your sock, or maybe they don't reach the back of you, so you can tuck it in your pants in back of you. If you are a large person you have lots of hiding places. I am quite thin, so I have a hard time getting a deck in.

If you are caught with it, don't let them have it! If they find it, act cool about it. Try telling them it's just a radio. They might buy it. If they say "let me see it" then show it to them, but don't let them handle it. Once they grab it, they won't give it back. So don't let them touch it, if they have a problem with it tell them you are taking it back to your car, then wait a while and try to go into a different entrance. If you make sure to watch the guards before you enter the arena, then you should be able to get it in with no problem.

If you are at a show where they are using metal detectors, or wands, you are fucked. You will have to be more drastic. I have heard of people using wheelchairs to get stuff in. The security never would think of searching a wheelchair real good, especially if you make yourself up to look like you are in really bad shape! I used this method once, and it was to get a camcorder into a show. I put it in the bottom case in a wheelchair that looked like it was electric, but it was gutted out so that there would be room. I was all wrapped up in blankets and made up with T-Shirts to match the band, buttons and banners, and drool. I was NOT making fun of handicapped people, I am not like that, but I was only using this method to get my camera in. It worked, too.

****
"I can't fucking breathe in here! There's SO much smoke!!
****

Now you should be inside. The hard part is over, well at least some of the hard stuff is. Now you have to locate yourself to get a good tape. A lot of people make the simple mistake of not being in the right place to get a good tape. Simply enough, the closer to the amps the better
. This is good because it reduces crowd noise. If you can adjust your deck, make sure you adjust the levels during the opening act. Never let the meters red line or you will get distortion. If you can, get a pair of the really small earphones, the ones that look like earplugs with wires. Then you can "practice" taping by taping the opening band in different places in the auditorium. Then before the main band comes on, review the tape and find out which placement has the best sound. It is important when making a good tape, to try to get as much stereo separation as possible. Often bands will pipe their instruments into the P.A. in stereo, so it is good to pick this up. When making the practice tape, talk into the mic so that you will know where you were. You only have to record in each spot for about 30 seconds. When you have found a good spot, then get ready for the main band!

Alright, one thing that is important about recording, microphone placement. Before you even go to the show you should know where and how you will place your microphones. If you have the two skinny ones I mentioned above, then you can do many things with them. A really good, and simple, place for them to go would be a hat. You just stick them in your hat poking out forwards, and you've got them lined up just where you are looking. The drawbacks to this are if you turn your head around then the sound will "sway" a little. Also, if you are short, you will hear the person behind you yelling at the top of their lungs. This isn't too good. But, if you are tall, or can stand on top of a chair the whole show, then cool. Another good place for mics is a banner. This is something that you have to plan ahead to do.

All you gotta do is make up a banner with the band's logo on it, like you see people waving around, and put it on some sort of pole. Ok, the banner will be strung across a T at the top of the pole. Then, you gotta wire in the microphones at either end of the T. This will result in great stereo, and barely any individual crowd noise. The crowd noise will sound like it should, far away, and only between songs. This method is one of the best for making a really good tape. Just be sure that if you try it that you find a place where when you put the banner up there aren't people behind you yelling for you to move it so they can see. So be sure to make it tall enough. I'll leave some creativity to you.

You should be able to find out how you like to hold the mics. There are many variations. If you are with a friend, then you can maybe hold one mic each in hats. This works good if you are standing together. You can get good stereo effect if you stand as far apart as the cords will let you.

Now, when you are making the tape, you should be timing from the point when you started it. Be sure that when it is near 30 minutes that you flip the tape very fast. Don't wait for the tape to end, then you will lost valuable time. The reason for this is because the leader tape is usually five seconds, and it takes about two or three seconds to flip the tape. Taking into account the leader tape on each side, you lose about 13 seconds if you wait till the end at least. So, before it gets to the leader, flip the tape. Then you lose maybe only four seconds maximum. You can also tell how close it is by looking at the spools and seeing how much tape is left on the small spool. If it is almost nothing, then flip the muther. Also, when you need to switch to another tape, get it out and ready to pop in so the transfer takes only a coupe seconds. Have the new tape forwarded past the leader so that you don't lose more time. As soon as you swap tapes, take the one that is full of the recordings, and pop out the tabs so that you don't fuck it up. It's easy to pop in the already used tape when flipping them like this. So take the precaution and pop out the tabs.

Now you should have a pretty good recording of the show, depending on all the things I mentioned above. Congratulate yourself on a job well done.

****

Flea Market Au Gratin...

****

You've got a really good tape now, and you want to know what the hell to do with it. Well the first thing you should do is make a copy for yourself to listen to. Don't use the originals to play all the time, especially if you are going to be listening to them in a car. When you make copies, make them on a good deck, or if you used fast speed on your recorder, then you have to use the recorder to make the copies. All this is common sense, so you should be able to make good copies.

Before you go and make copied for all your friends, make sure that there isn't any commercial value to this tape. If you know you can get some money for it, then only give a copy to friends that you can trust, because you don't want them to make the money themselves. It can sometimes be good to sell them at a record store on consignment. There are lots of record stores around that sell bootlegs. They are often ones that will say "collectors" or "used" records. Talk to them about the tape that you have. They will probally want to hear it. Make sure, though, that you trust them. You don't want them to buy one tape then turn around and make multiple copies for themselves to sell.

When you do something like sell a tape at a store, you will need to package it. Often, bootleg tapes are generic looking, with photo copied wrappers. If you make a nice looking package, then you can get more money for it. Also, it's a good idea to make the tape "limited", like only print up 100 or 200, etc. Or if you are going to making a lot, then make the first 100 "special" like make the wrapper color, or number them or something. Things like this are looked for by collectors. The only problem with tapes though is that they aren't too desirable by serious collectors unless they have a really good sound quality or are something unique. Say, for instance, that Blue Oyster Cult is playing a show and you go to tape it, and some nut jumps on stage and sets the singer's hair on fire, and as a result they play a 2 hour version of "Godzilla", then having this on tape will be VERY collectable. It is a bit extreme, but you can see what I mean. Also, it's good when the band mentions where they are at. Like on a Dio tape that I made he screams "It's great to be here in Lakeland Florida!!". Now something like that is cool because people in the area who saw the show would be interested in that tape because they were there and shit.

When you make the wrapper, you can use a copy machine if you don't care about color. It's good to make something that makes fun of the band. People who collect things of just a single band like to find unusual packaging. Find a picture of the band and mix it in with something that doesn't quite fit, like paste them into a picture with a bunch of naked gals. The more creative, the better. A good example of someone who has been exploited to the hilt is Frank Zappa. There are hundreds of Zappa bootlegs floating around. I know a few people who would pay $30.00 for one even if it's shit, just to have a copy.

Ok, that's tapes, what about albums? If you want to spend the money, you can have the tape pressed into vinyl. This can cost anywhere from a few hundred to a few thousand bucks. Most independant record factories will press an album without question. If they do have a problem, then make sure that you don't get the jacket printed there. Get them printed at a printer that you can trust. Bootlegs are very widespread now, and it can be quite easy to find a manufacturer that will press your tape into a record.

Records are what are most sought after by collectors. If you make a really good tape into some well made albums, then you can make some good cash. The same things that make tapes more desirable make records even more so desirable. Collectors love something "special", like limited edition fold out picture sleeves (expensive to make, but you can sell them for about $20-40.00 each). Also, colored vinyl is a good thing to do. Some of my favorite bootleg albums are on colored vinyl. I have a few that only the first 10-100 printed were on colored, the rest were on regular black. This is also a good idea to do if you want to make a really first quality bootleg.

Other things, when printing up the labels or sleeves, don't put your name one them! It's hard not to do, because you'd like to have your name known, but don't do it! Also, make sure you list all the songs on the outside of the album, so that when someone finds one, they will be more apt to purchase it because it has the songs they want. Make lots of liner notes about the show, and how the band was. "Rate" each song... people like a lot of shit on an album, and the more there is the better they are! It's really good if you have pics from the same concert too.

****

Lights!

****

What if you want to video tape? Well, it's harder, mainly because you can't slide a camcorder into your drawers, (at least not yet). So, you have to use other methods. One I mentioned before, a wheelchair. I think this is the best method, although you may think of something better or equal. If you are going to video, be sure that you have all the little lights taped off on the camera, they can be spotted easily by security. It's not like having a little deck that you can keep down, you will be holding the camera up to head level.

One thing I tried before was simple and effective. I put a wig on the camera, and went out into the field where the crowd was packed in tight. The camera looked like just another head from a distance, and since the security people don't like to get into the crowds, I was safe as can be. The only thing wrong with this was since there was a packed crowd around me, I was bumped a lot, which you don't want on video. You need to find a place that you can remain fairly still.

If you are doing video, make sure that you audio also. As long as you are sneaking in a big camera it won't be anything harder to get in your deck. So then afterwards if you have a stereo VCR, you can mix the sound in for top-quality audio! A video tape with stereo sound of a big band will get you anywhere from $50.00 to $300.00 a pop!

****
What the fuck?
****

Well, this has covered just about everything... but.. soundboard tapes. A soundboard tape is a tape that you record off of the soundboard! Simple, eh? These tapes are of the best quality of the band, but they lack crowd noise. If you can get the sound man to record a tape for you, cool, get it.

Soundboard recordings are much more rare than regular ones, so it's a good idea to try to get one.

When you go to a show, try to locate the sound guy. If you want, you can offer him money to record the show, or sometimes they will ask for drugs, etc. Sometimes, though, they will do it for free! I don't know if it's because they get pissed off at the bands, or don't care or what, but when it happens, it's good!

A lot of soundboards have a built in deck. If they got one of those just tell the guy you'd like to record with it, or else bring cables that you know will work in a board. This can be good, but if he records in the board, it may be an unusual tape speed, then you will have to locate someone with an appropriate deck later on. If you have the chance to get a board tape, get it, worry about computability later. If by good luck you can use the built in deck, that means that you can use your own deck to record the regular way, then you have two good, and different, tapes of the show!

When you listen to a soundboard tape, it's kind of boring. That's because there's no crowd noise, and no overdubs. It's a raw tape of exactly what is being pumped through the monitors. So, you can hear every little thing the band does, from missing a note to talking to each other between songs. Some people have taken a soundboard tape, and a microphoned tape and mixed them into one, so that you get soundboard quality with just a little bit of crowd noise to fill it out just right. This is a lot what bands do themselves when they make a live album. They record through the board, then add in cheering between the songs, and sometimes boost it during the songs. The only difference is that the bands will most likely put tons of overdubs and echo effects over the live stuff to make them sound better. That's why a good board tape is the ultimate!

****
Flip them burgers, hup, hup, hup!
****

Boy, aren't you hungry? But I bet that you don't have a bit of money on you. Sucks, doesn't it? Well, you don't have to go hungry.. all you need is a car and a little bit of guts.

This method of getting food for free is good when you are wanting food right then... you can't wait till you have money, etc., you have to eat NOW!

First, get in your car. You don't have one? Get a friend to drive, it doesn't matter, just make sure the driver is cool, because the driver usually has to do the work.

Then, go to your nearest drive-thru fast food place, and

enter the lane to get food. Now, I know you don't have money, but not to worry. Pull up to the ordering sign and wait.

"Can I take your order?" Blasting out of the speaker.

"Uh, hello, I was here about a half an hour ago and picked up food, and you forgot my -(fill in with what you want)-."

"Do you have a receipt?"

"It's in the bag."

If they continue to hassle you for a receipt, get angry. Tell them that this happens to you every fucking time you go there, and you are sick of it.

You had to drive all the way back to get the missing ________ and you aren't going to be satisfied unless you get what you want.

They should now give you the food that they supposedly forgot. This works good everywhere, because these shitholes have a policy that says that if someone says that they were shorted, they have to owe up. In short, "the customer is always right," even though you aren't a "real" customer.

When doing this, don't go overboard. Don't say that McDonald's forgot your Big Mac, your large fries, your 32oz Sprite, etc. Narrow it down to one or two items, preferably of the same ilk. Like go to Burger King and get the burgers, go across the street to Kentucky Fried Chicken to get the drinks, etc., etc.

This always works without a hitch, unless, and this is a big unless, you go to the same place and do it often until they can recognize you. Make a mental note of where you have been and be sure not to do it that often. It's good if you do it once on a Monday, and then the next time on a Friday, because the chances that you get the same good working the window is slim.

Ok, I am sure that if you run into any problems you should be creative enough to work them out. Just remember, their job is to serve you well, even if you are ripping them off (as long as they don't know that you are ripping them off) so don't ever back down once you start talking to them or you will "ruin" that place because they will surely remember you.

****

In a

land of spatted foil water bison...
****

You're sick to death of fast food and you want something good. Something expensive. But you still have not a cent to piss on. If you are determined enough, you can eat at any restaurant in your particular city, for free.

Requirements:

A phone
A nice set of clothes
An adult voice

These should be easy enough to come by, unless you are a kid, which fortunately enough forme, I'm not. So, round up these things and get ready.

Pick out a nice place to dine at and call them up.

(The following is a transcript from an actual call.)

RING RING RING

"__________ Restaurant, can I help you?"

"May I speak to a manager, please?"

"Yes, who may I say is calling?"

"______________" (Name left out coz I ain't that stupid, in this situation give them your REAL NAME)

"Just a second." Pause

"Hi, this is Rick, how may I help you?"

"Yes, this is __________, I was in your establishment the other night with a business associate of mine, and we went ahead and ordered, and when the food came out it was a bit cold."

"Oooo."

"Well, I understand that this happens every once in a while, it was quite busy that night. So we told the waiter and he took it back into the kitchen. Well, the problem is, when he brought it back, it was even colder than it was when we first got the food."

"That doesn't seem possible!"

"I know, that is what is so odd! I come into your restaurant very often, and this is the first time that this has happened. And to make things worse, the waiter didn't even act like anything was wrong. It was like he was totally indifferent to what was going on."

"What night was this?"

"This was Saturday night." (Use any night as long as it wasn't long ago, if you call Wednesday, tell them you were in on Monday, etc.)

"Well I was working that night, why didn't you ask to speak with a manager?"

"I would have liked to then, but as I said, I was with a business associate of mine, and it was really an embarrassing situation. I didn't want to make things worse by causing a scene. I wasn't even going to call at all but I really feel bad about what happened, I mean I have recommended your establishment to several colleagues of mine, and I can't just write this one off."

"I know how you feel."

"Well, I would just like to know what you could do to make me want to come back to your restaurant, after all, I'd hate to see you lose a reputable customer."

"Oh, I don't want to lose a reputable customer! Tell you what, how would you like to come in sometime this weekend?"

"Well, I am free on Friday night." (Or any night that you deem necessary.)

"Ok. Come in Friday night with your associate, and ask for Rick. I'll make sure that your meal is perfect, and I'll pick up the tab."

"Rick, that would be great! I really appreciate this."

"Well, like I said, I'm sorry this had to happen, and don't want to lose good customer."

"Thank you very much, see you Friday night."

"Ok, good-bye."

"Bye."

We went in that Friday, and ate a rather large meal on the house, not including alcoholic beverages (something about the law).

One of the keys to doing this successfully is to be nice. Don't get too angry with the managers of these places or you will not fit the image you want to project. The last thing these guys want to do is give a free meal to an asshole. But, if you call up and just act dissappointed in the service, food, etc., then they will glady help you out.

Another point which is very important, is never, NEVER ask for a free meal outright! Always make them offer it. You can't get in trouble for complaining. Just use the line, "What can you do to make me come back?" Or: "What can you do to make me happy?" This way insures that you are not trying to just "freeload" in the eyes of Johnny Law.

As with the fast food Bernsteining, don't do this too often. The word may get around. Plus, you don't want to "burn out" your area. Once you do it at one place, you can't do it there again for a long time (unless you know they got a new manager, etc).

Also, above, in the transcript, I said to use your real name. Why lie? You can't get into any trouble! Plus, some restaurants will just send you out a gift certificate. Whenever I go to a place, I leave a nice tip (that's right I tip!) and my business card. This makes them feel good for doing it. You never want to let them know that you are scamming them.

I. CON JOBS

New York City (My Home!) is the leader in ATM con jobs. Altogether, about 2,000 Citibank users were victimized by ATm con artist in one years time for a tune of $495,000!!So I'm going to spread some light on what and how these cons are pulled off.

Method 1: THE "DEFECTIVE ATM" CON

A con method popular with Citibank ATMs netted one con artist $92,000- with the unwitting assitance of his 374 victims. The scheme works in lobbies with more than one ATM, and a service phone. The well dressed and articulate con man poses as a legit user and stands between two ATMs, pretending to be talking to the bank service personnel over the service phone. After a user inserts his card into the ATMs card reader slot he tells his that the machine is not working. The user withdraws his card leaving the ATM activated. THe con man then observes theuser enterring his PIN into the adjecent ATM. Then, still holding the phone, the con man enters the users PIN into the first ATM. In make-believe conversation with the bank, the con man acts like he is receiving instructions from the bank. To complete the theft he talks the user (major social engineering!) into entering his card into the first ATM again to "test" or "clear" the ATM. He claims that bank personnel think that the user's card "locked up" or "jammed" the ATM and or that ATM may have made the users card defective, and the insertion of it is required to "unlock" or "unjam" the ATM and/or to verify that the user's card is still vaild. After the users leaves, the con manenters into the keypad and withdraws the maximum daily amount from the users account.

This only works on Citibank ATMs cause they don't take the users card, but once the card is slipped in the ATM is activated.

Method 2. PHONE PIN-EXTRACTION SCAMS

Another popular con is for the con man to call up an ATM user whose card he's found or stolen. He identifies himself as a police officer, and obtains the PIN from the user by stating that it is required by law to verify the card owner. This works really well if you can bullshit them good like act like you have to do something and tell them to call you right back (on a loop!) and have a friend answer as the police station!

Method 3. THE BANK DICK CON

A subject was recently was recently convicted in N.Y. and Boston of defrauding ATM accounts of $150,000. He dubed over 300 ATM users into believing he was a bank security officer who needed assistance in the apprehending of a dishonest bank employee. The users were convinced to leave their bank cards under the locked door of the bank. The con man would then "fish" the cards out. The next morning the con man would have someone make a phone call to the card holder saying that they have caught the employee and dective "hacker" would like to thank you to. But since the employee did come is contact with there card the bank is going to give them a new PIN # after the get the old one! Then the con man's helper would say come pick up your new card and we will tell you your new PIN #.

II. Physical Methods

Some folks just dont like to outsmart a system or person. They prefer the more physical approach by either breaking or removing the ATM. The hazards are obvious-several built-in silent alarms,heavy stainless steel safe like construction, the amount of commotion and noise that results from their efforts, hard to dispose of evidence, etc. Those who have the most success with physical methods, plan and execute their operation as if it were commando mission.

The methods described below can also be used on night depositories, payphones, dollar changers, candy machines, parking meters,etc. Physical attacks must be completed within 10 minutes as ATMs abound with vibration, heat and proximity detectors, and most are silent.

To defeat any internal alarm mechanism,refer to the phone tapping approach (described in detail later) that hooks-up both the ATM and main computer to a programmed micro. So while Hood one is ripping-off or -up the ATM, the micro is whispering sweet nothings to the main computer. NOTE that not all ATM alarms transmit thru the ATM como lines, particulary with thru-the-wall ATMs. To minimize the noise and commotion, heavy blankets(used by movers) can be drapped over the ATM.

Method 1. SUPER COLD GASES

Liquid nitrogen can be used. It is simply poured onto or into the offending part of the ATM and when it hits 100 degrees or so, a sledge or a ballpeen hammer is smartyl slammedin to. THe metal SHOULD shatter like glass. Then one just simply reaches in and examines the untold riches stored inside. Super-cooled gases can also wreck havoc on electronics, cameras and films, and bullet-proof glass, and can be purchased from suppliers of medical and chemical supplies.

Method 2. WATER & ICE

We have also herd that pouring warm water into an isolated ATM on a very cold night is effective. When water freezes, it expands with a terrific force, and will shatter or tear apart anything made by man. The water is poured or pumped in thru the card slot or cash dispenser. It is heavily mixed with wood shavings or fiberglass to stop-up any drainage hole in the ATM. Leaks can also be plugged up with window putty or bubble gum.

Method 3. MORE FREEZE METHODS

ATMs use ACE locks (the ones found on most vending machines, the circle type lock) Freon works on these locks. Somw outlaws empty a can of freon into an ATM lock, pound a screwdriver into the key way, and wrench the lock out. And motor-driven ACE lock pick will vibrate pins into the right positions withine a few minutes. The ACE lock picks can be aquired from STEVE ARNOLDS GUN ROOM call (503)726-6360 for a free catalog they have a-lot of cool stuff!

Method 4. ACETYLENE & DRILLS

ATMs are notorisly vulnerable to attacks using acetylene torches. With most ATMs no more than 5 minutes are required for the entire job! And most ATMs can be drilled out in under 15 minutes, using carbide bits and high rpm drills (check on my SAFECRACKING text to see more about drilling.).

Method 4. SHAPED CHARGES

Placing shaped charges on each support and detonating them all at the same time liberates the ATM. You can firgue this out by yourself.You can also check most BBS's to find out how to make explosives but I wouldn't recommed it, since most of the expolsive files I've seen are inaccurate and leaves out MAJOR measurements and cautions! Your best best is to use black powder that you can get form almost all gun stores.

Method 5. BLOCKING THE DISPENSER

Some ATMs use money drawers. The ATM outlaw screws or epoxies the drawer solidly shut, at the onset of a busy three-day holiday. At the end of each night he returns and he removes the money by unscrewing or with a hammer & chisel, shatter the epoxy bond.

III. ELECTRONIC & COMPUTER SCAMS

Scarcely a week goes by that I don't hear about one scheme or another successfully used by phreaks & hackers to penetrate large systems to access data banks and to perform various manipulations.

Although we have only been able to verify one or two of the methods that we will discribe, numerous cases have arisen in recent years in which an ATM was defrauded with no evidence of a hardware or software bug to account for the robbery.

The outlaw can use several approaches. One is to use wiretapping. Another is to obtain the secrets of the cipher, or hardware or software defeats to the system and proceed accordingly. Another one that works with banks is to set up phony debit accounts and program the computer to beleive that the debit accounts are full of money. Then when a three day weekend comes around proceed with friend to deplete all of these debit accounts by making various rounds to ATMs.

Electronic frauds of ATMs require an excellent technical understanding of phone and-or computers all of which you can obtain from worthy underground news letters such as TAP, and 2600, etc. OR from a H/P BBS.

"Tapping" or "wiretapping" consists of the unauthorized electronic monitering of a signal (voice or digital) transmitted over a phone or computer (commo) circuit. A "tap" is the monitoring device that does this. Athough a tap is usually placed somewhere on a phoneline or junction box, it may be placed inside of a phone, modem or computer.

With the advent of isolated stand-alone ATMs (with vulnerable phone lines, including POS terminals) and computer technology. The phone circuits that connect ATMs to their host computer (located in the banks data processing center) can be tapped anywhere between the two.

An "invasive tap" is one in which a hard electronic connection is made between the tap and the commo circuit. A "non-invasive" tap is one in which an induction loop or antenna is used to pick up the EMI generated by the signal, and there is no physical connection between the commo circuit and the line.

A "passive tap" is one in which the tap simply tramits to a recorder or directly records the tapped signal and in no way interfers with it. An "active tap" is one in which the tap ALSO interferes (changes,adds to or deletes) the tapped signal in some way. Active taps are more sophisted. A typical ATM active tap is one that records a signal, the later plays it back over the line.

Be sure to look for my text "HIGH TECH TOYS" it lists were to get things that are VERY hard to get or things that you may need a license to obtain without those hassles all you need will be money!

Method 1. PASSIVE TAPS

All tapped ATM transactions are recorded over a period of time (but not interfered with). Once the serial protocal and MA codes are understood, the transmitted data is decrypted (if encrypted) using known entry data to the ATM. Note that some systems use a MA code that is complex and very difficult to crack.

Messages to and from the ATMs host computers are composed of various fields. One field identifies the transaction type, one the PIN, one the PAN, one the amount, one the approval code, one the transaction number and perhaps other fields. In most systems, either nothing is encrypted or only the PIN field. In others, the entire message is encrypted.

The ATM/host circuit is monitored over a period of time to deterive PINs,PANs and other entry data of other ATM users based upon (decrypted) transmitted data. Phony debit cards are then made to defraud ATM accounts with known PINs and PANs.

Method 2. ACTIVE TAPS

Active tapping is one method of spoofing. The c4ritical part of the host computer's message are the approval and amounts fields. The critical parts of the ATMs transmission are the continuous transmission it makes to the host computer when NO one is using it to indicate that it is OK, and the PIN and amount fields. Booth good and bad cards and good and bad PINs are entered at various times and days to differentiate between the various massage components. Various quiescent periods is also recorded.

Once the message structures are understood, a computer is then substituted to act as both the host computer and the ATM. That is, a computer is then connected between the ATM and the host computer. This computer acts like the host computer to the ATM, and like the ATM to the host computer.

An accomplice uses the ATM to go thru the motions of making legitimate transactions. If his procedures are correct, the ATM communicates, with the host computer for permission to discharge the money. Several methods:

(A) The phreaker changes the approval field in the hosts message to OK the transaction regardless of its real decision. The phreaker may interdict the message regardless of iits real decision. The phreaker may interdict the message from the ATM to tell the host that the ATM is inactive while it interdicts the host message to tell the ATM to disburse the cash. Since the ATM is no longer connected to the host computer, and the host computer believes that it is talking to an unused ATM (or one engaged in balance inquiry transaction), no monies will be deducted from any debit account, no denials will be made based upon daily maximum limits, and no alarm will be sounded due to suspicious behavior. Even if the ATM sounds an alarm, the host computer wont hear it as long as the phreaker is whispering sweet nothings into its ear. Also by using this method, as long as the PIN & PAN check digits are legitimate ones based upon the ATMs preliminary and cursory checks, the PINs and PANs themselves can be phony because the host won't be there to verify legitimacies! That is no legal PINs and PANs need be known nor the algorithm for encrypting PINs.

(B) The ATMs message is replaced by a previously recorded legitimate transaction message played back by the phreaker. The cash is despense as before. The play back method won't work if the encryption or MA process embed a transaction, clock or random code into the message, making all messages unique.

(C) The phreaker/hacker changes the PIN field in the ATMs message to a legitimate PIN of a fat-cat like DONALD TRUMPs account. The phreaker/hacker then withdraws someone else's money.

(D) The phreaker/hacker changes the amount field in the ATMs message to a much lower one, and then changes the amount field in the host's message back to the higher amount (debit transactions- the opposite changes are made for credit transactions). Sooo the phreaker can withdraw $200 from his account with only $10 actually debited from it by the host. He can then make many withdrawals before the host cuts him off for exceeding the daily max.

Method 3. TEMPEST IV

A thin induction pick-up coil, consisting of many turns of one thickness of #28 or thinner enamel wire sandwiched between two self-adhesive labels, no larger than a debit card, can be inserted at least part way inside the card slot of most ATMs. This coil is then used to "listen in" on the electrical activity inside of the ATM to try to determine which signals control the release of money. Using this same coil as a transmitter anteenna, these signals are then transmitted ti the realse logic to activate it.

It is believed that a thin coil about the size of a dime can be maneuvered quite a ways inside most ATMs for sensing purpose, and that small metal hooks have also been fed into ATMs to obtain direct hookups to logic and power circuits.

It is believe that some outlaws have obtained ATM cards. They then machined out the inside of the cards, except the magnetic strip. They then place flat coils inside the machined out area. They then monitor the coils during legitimate transactions. They can also use the coils to transmit desired signals. This is kind of the method used in TERMINATOR 2.

IV. BOGUS CARD, GETTING PINs

Almost all credit cards now come with either a hologram or an embedded chip ("Smart Card"), and are thus nearly impossible to counterfeit to date. However, since most debit cards are not optically read by ATMs, they are much easier to counterfeit. To counterfeit a card the following is needed:

(1) A card embosser, which can be readily obtained from commercial sources (see "Embossing Equipment and Supplies" or similar in the Yellow Pages) without question asked. A used, serviceable embosser ran use $210 + shipping & handling. (2) A magnetic stripe decoder/encoder (skimmer), which can be purchased from the same company as the embossing equipment or just look in the back of Computer Magazines. (3) PIN checkers are not known to be available to the general public. However, if one were stolen, the user could guess at card PINs by trial-and-error effort based upon the knowledge of how PINs are derived. (4) PANs,PINs and ciphers, which can be obtained from a number of ways usually involving theft. About 50% of ATM users write their PINs either on their debit card or somewhere in there wallet or purse. And most user-chosen PINs are easily guessed. The encrypted PINs can be directly lifted or read from the magnetic stripe, and the encryption scheme determined by comparing the encryption with the known PIN # of a dozen or so cards.

Deposits on ATM:

Various banks have various systems. As an example, at CITIbank a deposit was made to a specific account. Your account was updated with a MEMO update, i.e. it would show up on your balance. However it did not become AVAILABLE funds until it was verified by a teller. On the envelope was Customer ID number, the envelope number and the Entered dollar amount, the branch # and the Machine #.

There was also a selection for OTHER PAYMENTS. This allowed you to dump any deposit into the ATM.

What are you assured then when you deposit to an ATM ?

1) You have a banking RECORD (not a reciept at Citibank). If you have this record, there is a VERY high percentage that you deposited something at that ATM.

2) Some banks have ways of crediting your deposit RIGHT NOW. This could be done by a balance in another account (i.e. a long term C.D. or a line of credit.) That way they can get you if you lied.

************** ATM Splitting a Card in half ***************

I've worked with about 75% of the types of machines on the market and NONE of them split a card in half upon swallow. However, some NETWORKS have a policy of slicing a card to avoid security problems.

Trusting an ATM.

Intresting you should bring this up, I'm just brusing up a paper describing a REAL situation where your card and PIN are in the clear. This involves a customer using a bank that is part of a network. All the information was available to folks in DP, if they put in some efforts to get it.

Mis-Implementation of an ATM PIN security system

1. Synopsis

In an EFT (Electronic Funds Transfer) network, a single node which does not implement the proper security can have effects throughout the network. In this paper, the author describes an example of how security features were ignored, never-implemented, and/or incorrectly designed. The human factors involved in the final implementation are explored by showing several major vulnerabilites caused by a Savings and Loan and a regional EFT network's lack of vigilance in installing an EFT network node. While using an EFT system as an example, the concepts can be extrapolated into the implementation of other secured systems.

2. Background

A small Savings and Loan was setting up a small (10 to 16 ATMs) proprietary Automatic Teller Machine (ATM) network. This network was then intended to link up to a regional network. The manufacturer of the institution's online banking processor sent an on-site programmer to develop the required interfaces.

An ATM network consists of three main parts. The first is the ATM itself. An ATM can have a range of intelligence. In this case the ATM was able to decode a PIN (Personal Identification Number) using an institution supplied DES (Data Encryption Standard) key. It was then required to send a request for funds to the host where it would receive authorization.

The second portion of the network is the ATM controller. The controller monitors the transaction, and routes the message to the authorization processor. The controller would also generally monitor the physical devices and statuses of the ATM.

The third portion of the network is the authorization system. In this case customers of the local institution would have the transaction authorized on the same processor. Customers from foreign (i.e. one that does not belong to the institution that runs the ATM) institutions would be authorized by the regional network. Authorization could be from a run-up file which maintains establishes a limit on withdrawals for a given account during a given period. A better method is authorization direct from the institution which issued the card.

3. Security

The system has a two component key system to allow access to the network by the customer. The first is the physical ATM card which has a magnetic stripe. The magnetic stripe contains account information. The second component is the Personal Identification Number (PIN). The PIN is hand entered by the customer into the ATM at transaction time. Given these two parts, the network will assume that the user is the appropriate customer and allow the transaction to proceed.

The Magnetic stripe is in the clear and may be assume to be reproducible using various methods, thus the PIN is crucial security.

Security

PIN security

3.1. PIN security

3.1.1. PIN key validation method

PINs can be linked up to a particular card in a number of ways. One method puts the PIN into a central data base in a one-way encrypted format. When a PIN is presented, it would be encrypted against the format in the data base. This method requires a method of encrypting the PIN given at the ATM, until it can be verified at the central site. Problems can also occur if the institution wants to move the PIN data base to another processor, especially from a different computer vendor.

Another method is to take information on the card, combine it with an institution PIN encryption key (PIN key) and use that to generate the PIN. The institution in question used the PIN key method. This allows the customer to be verified at the ATM itself and no transmission of the PIN is required. The risk of the system is the PIN key must be maintained under the tightest of security.

The PIN key is used to generate the natural PIN. This is derived by taking the account number and using DES upon it with the PIN key. The resulting number then is decimialized by doing a lookup on a 16 digit decimalization table to convert the resulting hexadecimal digits to decimal digits. An ATM loaded with the appropriate PIN key can then validate a customer locally with no need to send PIN information to the network, thereby reducing the risk of compromise.

The PIN key requires the utmost security. Once the PIN key is known, any customer's ATM card, with corresponding PIN can be created given a customer account number. The ATM allows for the PIN to be entered at the ATM in two parts, thus allowing each of two bank officers to know only one half of the key. If desired, a terminal master key can be loaded and then the encrypted PIN key loaded from the network.

The decimalization table usually consists of 0 to 9 and 0 to 5, ("0" to "F" in hexadecimal where "F" = 15). The decimalization table can be put into any order, scrambling the digits and slowing down an attacker. (As a side note, it could be noted that using the "standard" table, the PIN digits are weighted to 0 through 5, each having a 1/8 chance of being the digit, while 6 through 9 has only a 1/16 chance.)

When handling a foreign card, (i.e. one that does not belong to the institution that runs the ATM), the PIN must be passed on to the network in encrypted form. First, however, it must be passed from the ATM to the ATM controller. This is accomplished by encrypting the PIN entered at the ATM using a communication key (communication key), The communication key is entered at the ATM much like the PIN key. In addition, it can be downloaded from the network. The PIN is decrypted at the controller and then reencrypted with the network's communication key.

Security

PIN security

PIN key validation method

Maintaining the the security of the foreign PIN is of critical importance. Given the foreign PIN along with the ATM card's magnetic image, the perpetrator has access to an account from any ATM on the network. This would make tracking of potential attackers quite difficult, since the ATM and the institution they extract funds from can be completely different from the institution where the information was gleaned.

Given that the encrypted PIN goes through normal communication processes, it could be logged on the normal I/O logs. Since it is subject to such logging, the PIN in any form should be denied from the logging function.

3.2. Security Violations

While the EFT network has potential to run in a secured mode given some of the precautions outlined above, the potential for abuse of security is quite easy. In the case of this system, security was compromised in a number of ways, each leading to the potential loss of funds, and to a loss of confidence in the EFT system itself.

3.2.1. Violations of the PIN key method

The two custodian system simply wasn't practical when ATMs were being installed all over the state. Two examples show this: When asked by the developer for the PIN key to be entered into a test ATM, there was first a massive search for the key, and then it was read to him over the phone. The PIN key was written on a scrap of paper which was not secured. This is the PIN key that all the customer PINs are based on, and which compromise should require the reissue of all PINs.)

The importance of a system to enter the PIN key by appropriate officers of the bank should not be overlooked. In practice the ATM installer might be the one asked to enter the keys into the machine. This indeed was demonstrated in this case where the ATM installer not only had the keys for the Savings and Loan, but also for other institutions in the area. This was kept in the high security area of the notebook in the installer's front pocket.

Having a Master key entered into the ATM by officers of the bank might add an additional layer of security to the system. The actual PIN key would then be loaded in encrypted form from the network. In the example above, if the installer was aware of the terminal master key, he would have to monitor the line to derive the actual PIN key.

The use of a downline encrypted key was never implemented, due to the potential complications and added cost of such a system. Even if it was, once violated, security can only be regained by a complete reissue of customer PINs with the resulting confusion ensuing.

Security

Security Violations

3.2.2. Network validated PIN Security violations

Given the potential for untraced transactions, the maintenance of the foreign PINs security was extremely important. In the PIN key example above, any violation would directly affect the institution of the violators. This would limit the scope of an investigation, and enhance the chance of detection and apprehension. The violation of foreign PIN information has a much wider sphere of attack, with the corresponding lower chance of apprehension.

The communication key itself was never secured. In this case, the developer handed the key to the bank officers, to ensure the communication key didn't get misplaced as the PIN key did (This way he could recall it in case it got lost). Given the communication key, the security violation potential is simple enough. The programmer could simply tap the line between the ATM and the controller. This information could then generate a set of PIN and card image pairs. He would even have account balances.

Tapping the line would have been an effort, and worse yet he could get caught. However, having the I/O logs could serve the same purpose. While originally designed to obscure PIN information in the I/O logs, the feature was disabled due to problems caused by the regional network during testing. The I/O logs would be sent to the developer any time there was a problem with the ATM controller or the network interface.

The generation of PIN and card image pairs has a potential for even the most secured system on the network to be attacked by the lapse in security of a weaker node. Neither the communication key, nor the PIN should ever be available in the clear. This requires special hardware at the controller to store this information. In this case, the institution had no desire to install a secured box for storing key information. The communication key was available in software, and the PIN was in the clear during the process of decrypting from the ATM and re-encrypting with the network key. Any programmer on the system with access to the controller could put in a log file to tap off the PINs at that point.

The largest failure of the system, though, was not a result of the items described above. The largest failure in the system was in the method of encrypting the PIN before going to the network. This is due to the failure of the network to have a secured key between sites. The PIN was to be encrypted with a network key. The network key was sent in encrypted form from the network to the ATM controller. However, the key to decrypt the network key was sent almost in the clear as part of the start-of-day sequence.

Any infiltrator monitoring the line would be able to get all key information by monitoring the start-of-day sequence, doing the trivial decryption of the communication key, and proceeding to gather card image and PIN pairs. The infiltrator could then generate cards and attack the system at his leisure.

Security

Security Violations

Network validated PIN Security violations

The network-ATM controller security failure is the most critical feature since it was defined by a regional network supporting many institutions. The network was supposedly in a better position to understand the security requirements.

4. The Human Factors in Security Violation

It is important the users of a system be appraised of the procedures for securing the system. They should understand the risks, and know what they are protecting. The bank officers in charge of the program had little experience with ATM systems. They were never fully indoctrinated in the consequences of a PIN key or communication key compromise. The officers showed great surprise when the developer was able to generate PINs for supplied test cards. Given the potential risk, nothing more was done to try to change the PIN key, even though, they were quite aware that the PIN key was in the developer's possession. They once even called the developer for the PIN key when they weren't able to find it.

The developer had a desire to maintain a smooth running system and cut down on the development time of an already over-budget project. Too much security, for example modifying I/O logs, could delay the isolation or repair of a problem.

The regional network was actually a marketing company who subcontracted out the data processing tasks. They failed to recognized the security problem of sending key information with extremely weak encryption. The keys were all but sent in the clear. There seemed to be a belief that the use of encryption in and of itself caused a network to be secured. The use of DES with an unsecured communication key gave the appearance of a secured link.

The lack of audits of the system, both in design and implementation was the final security defect which allowed the system to be compromised in so many ways. An example of the Savings and Loan's internal auditors failure to understand the problems or technology is when the auditors insisted that no contract developers would be allowed physically into the computer room. The fact was, access to the computer room was never required to perform any of the described violations.

5. Security Corrections

As in any system where security was required, the time to implement it is at the beginning. This requires the review of both implementation and operational plans for the network. Audits should be performed to verify that the procedures are followed as described in the plan. Financing, scheduling and man power for such audits must be allocated so security issues can be addressed.

For this institution, the first step would have been to indoctrinate the banking officers of the risks in the ATM network, the vulnerabilites, and the security measures required.

Custodians of all keys should be well aware of their responsibilities for those keys. A fall back system of key recovery must be in place in case an officer is not available for key entry.

The cost of installing hardware encryption units at the host should be included in the cost of putting in the system. The host unit could generate down-line keys for both the PIN key and the communication key thus making it more difficult to derive these keys without collusion from at least three people.

A secured communications key should be established between the Network and the institution. This would allow for the exchange of working communication keys. This key should be changed with a reasonable frequency.

All these areas should be audited in both the system specification and implementation to make sure they are not being abridged in the name of expediency.

6. Summary

In this view of a single institution, a number of failures in the security system were shown. There was shown a definite failure to appreciate what was required in the way of security for PINs and keys used to derive PIN information. An avoidance of up front costs for security lead to potentially higher cost in the future. The key area was the lack of audits of the EFT system by both the institution and the network, causing potential loss to all institutions on the network.

<-> Credit Carding <->

There are at least three types of security devices on credit cards that you aren't supposed to know about. These are the account number, the signature panel, and the magnetic strip.

The Account Number

A Social Security card has nine digits. So do two-part Zip codes. A domestic phone number, including area code, has ten digits. Yet a complete MasterCard number has twenty digits. Why so many?

It is not mathematically necessary for any credit-card account number to have more than eight digits. Each cardholder must, of course, have a unique number. Visa and MasterCard are estimated to have about sixty-five million cardholders each. Thus their numbering system must have at least sixty-five million available numbers.

There are one hundred million possible combinations of eight digits --- 00000000, 00000001, 00000002, 00000003, all the way up to 99999999. So eight digits would be enough. To allow for future growth, an issuer the size of Visa or MasterCard could not opt for nine digits-- enough for a billion different numbers.

In fact, a Visa card has thirteen digits and sometimes more. An American Express card has fifteen digits. Diners Club cards have fourteen. Carte Blanche has ten. Obviously, the card issuers are projecting that they billions and billions of cardholders and need those digits to ensure a different number for each. The extra digits are a security device.

Say you Visa number is 4211 503 417 268. Each purchase must be entered into a computer from a sales slip. The account number tags the purchase to your account. The persons who enter account numbers into computers get bored and sometimes make mistakes. They might enter 4211 503 471 268 or 4211 703 417 268 instead.

The advantage of this thirteen-digit numbering system is that it is unlikely any Visa cardholder has 4211 503 471 268 or 4211 703 417 268 for an account number. There are 10 trillion possible thirteen-digit Visa numbers (0000 000 000 000; 0000 000 000 001........9999 999 999 999). Only about sixty-five million of those numbers are numbers of actual, active accounts. The odds that an incorrectly entered number would correspond to a real number are something like about 1 in 150,000.

Other card-numbering systems are even more secure. Of the quadrillion possible fifteen-digit American Express card numbers, only about 11 million are assigned. The chance of a random number happening to correspond to an existing account number is about 1 in 90,000,000. Taking all twenty digits on a MasterCard, there are one hundred quintillion (100,000,000,000,000,000,000) possible numbers for sixty-five million cardholders. The chance of a random string of digits matching a real MasterCard number is about one in one and a half trillion.

Among other things, this makes possible those television ads inviting holders of credit cards to phone to order merchandise. The operstators who take the calls never see the callers' credit cards nor their signatures. How can they be sure the callers even have credit cards?

They base their confidence on the security of the credit card numbering systems. If someone calls in and makes up a credit card number, the number surely won't be an existing credit card number. The deception can be spotted instantly by plugging into the credit-card company's computer. For all practical purposes, the only way to come up with a genuine credit-card number is to read it off a credit card. The number, not a piece of plastic is enough.

Signature Panel

You're not supposed to erase the signature panel if you steal a card! You might be thinking that you could just write the cardholder's name on the panel. You're thinking that this would be great if you were going to withdraw some cash from the bank, for they make you sign a slip and it must match up to the signature on the card. If you or anyone else does this, you will soon find the card completely worthless (at least it can not be shown).

Some credit cards have background design that rubs off if anyone tries to erase the signature. There's the "fingerprint" design on the American Express panel, repeated Visa or MasterCard logos on some bank cards, and the "Safesig" design on others. The principle is the same as with the security paper, the wavy-line pattern erases, leaving a white area. This makes it obvious that the signature has been altered.

There is a more elaborate gimmick in credit-card panels. It is said that if you erase the panel, a secret word, "VOID", appears to prevent use of the card. The Administration has taken 15 common credit cards and sacrificed them to test this theory.

The odinary pen eraser will erase credit-card signature panels, if slowly. The panels are removed pretty easy with a cloth and Energine. This method disolves the panels cleanly. Of the 15 cards tested, 6 had nothing under the panel (other than a contiuation of the cards back design where there was one). Nine cards had the words "VOID" under the panel. In all cases, the VOID's were printed small and repeated many times under the panel.

<-><-><-><-><-><-><-><-><-><-><-><-><-><-><->
<-><-> This is How They Ranked <-><->
<-><-><-><-><-><-><-><-><-><-><-><-><-><-><->

Cards with VOID Devices

Bloomingdale's
Bonwit Teller
Bullock's
Chase Convenience Banking Card
First Interstate Bank Card
I. Magnin
Joseph Magnin
Montgomer Ward
Visa (Chase Manhattan)

Cards without VOID Devices

- American Express Gold Card
- Broadway
- MasterCard (Citibank)
- Neiman-Marcus
- Robinson's
- Saks Fifth Avenue

When held to a strong light, the VOIDs were visible through the Bloomingdale's even without removing the panel.

The Way Around this Security!

There is but one way we could think of getting around this feature... painting over the panel! This would work only if the card didn't have a design on the panel. Cards that have a difficult color to match would be near immpossible also (Saks' panel is greenish-tan khaki color).

The Magnetic Strip

One of the last security devices is on the back, the brown magnetic strip. You probably think that there are sun-dry personal details about the cardholder stored in the strip. The strip is really no more information capacity than a similar snippet of recording tape. For their part, banks are reticent about the strip.

The strip need not contain any information other than the account number or similer identification. Any further information needed to complete and automatic-teller transaction --such as the current account balances-- can be called up from bank computers and need not be encoded in the strip.

Evidently, the card expiration date is in the strip. Expirated cards can be "eaten" by automatic-teller machines even when the expired card has the same account number and name as its valid replacement card. Credit limit, address, phone number, employer, ect., must not be indicated in the strip, for banks do not issue new cards just because this information changes.

It is not clear if the personal indentification number is in the strip or called up from the bank computer. Many automatic teller machines have a secret limit of three attempts for providing the correct personal identification number. After three wrong attempts, the "customer" is assumed to be a crook with a stolen credit card and the card is "eaten".

It is possible to scramble the information in the strip by rubbing a magnet over it. Worker's in hospitols or research facilities with large electromagnets sometimes find their cards no longer work in automatic-teller machines.

The Bloomingdale's Color Code

Only in a few cases does the color of the credit card mean anything. There are the American Express, Visa, and MasterCard gold cards for preferred customers. The Air Travel Card comes in red and green, of which green is better. The most elaborate color scheme, and a source of some confusion to status-consious queues, is that of Bloomingdale's credit cards. The five colors of Bloomingdale's cards do not signify credit limits per se, but they do tip off the sales staff as to what type of customer you are. According to Bloomingdale's credit deptpartment, here is how it works: Low color in pecking order is blue, issued to Bloomingdale's employees as a perk in their compensation packages. The basic Bloomie's card is yellow. Like most department store cards, it can be used to spread payments over several months with the payment of a finance charge. The red card gives holders three months' free interest and is issued to customers who regularly make large purchases. The silver card is good for unlimited, but as with a travel and entertainment card, all charges must be paid within thirty days. The gold card offers the same payment options as the yellow card, but is reserved for the store's biggest customers.

<-> The Dropsite <->

The Dropsite

You must find a place for all of these "goodies" to go. If you really wanted to get in deep, you might have them sent to your house. You may also have a crude enemy in mind. Stop and think of the benifits from this suggestion.

To get a sufficient drop, you have to find a deserted house. It must look like it is lived in though, grass mowed, drapes, ect. When you are ready to order this stuff, have it sent overnight UPS and leave a note on the door saying that you work acquard hours and to leave it on the back porch. This is really the best way to do it, but I will tell you about a few others.

U-Haul has what is called "Rent a Spot". Anything sent to this "spot", U-Haul has to sign for. You and only you can get anything sent there. You might be able to send the "goodies" there and then cancell the "spot" after they arrive. This is very tricky and I would not recomend it, but then again, there may not be a vacant house where you live.

This drop is just a house with people in it you do not know and who would not recognize you if seen again. Just have the packages sent there. Phone and tell them that you ordered a package and it was sent to the wrong house. Tell them that you will pick it up when sometime after it arrives if they don't mind. I strongly disencourage this method.

Another drop could be any video or computer retail store. Here is a little dialog that might explain this a little better:

You: Hi, this is David Lightman. I am interested in your new Sanyo computer system. I would like to talk to someone about this.

Worker: Sure. Let me tell you all about it.

(For the text on Sanyo, please write them. I am too lazy)

(Continued)

You: Well, it sounds like just what I have been looking for. Could I buy it now with my Visa and have my nephew pick it up later? I am sick and can't get out.

Worker: Sure. I guess so.

ect. ect. ect...

You just pick up the package later by telling the guy your name and what you need to get. Free shit. Already paid for.

Ordering Mechandise

Don't try this if you have a high voice! One exception to this though, you might want to fake it like a lady.

Some of the best places to get stuff from is advertizements in magazines. When you do this, try to schedual it at the begining of the month, after the bills have been sent. This will provide you for more time for unexpected misshaps that might occur. You must be sure that this is going to work, or just pull out imediately! When you call the merchant, try to make it at night or late in the day. Most operators are very tired then and not really thinking of what they are doing. Make sure you know exactly it is you want and everything about card by memory if asked.

When you finally get your packages, completely forget where the drop was, for you will NEVER want to use the same one again.

One more thing, the insurance companies pay for all stolen goods gotten by credit cards.

```
<->   This article was written for  <->
<-> informational purposes only.    <->
<-> All of it's content can not     <->
<-> be held directly or indirectly  <->
<-> if a violation of the law       <->
<-> occurs.  I, nor any member of   <->
<-> The Administration can be held  <->
<-> responsible if a violation of   <->
<-> the law occurs.  We do not in   <->
<-> any way promote the use of      <->
<-> stolen credit cards.            <->
<->                                 <->
```

: How to build a Bug Detector :

][][][
Basic theory
][][][

Because most bugs are triggered through certain frequencies, it is very simple to build a small sweeping device that will trigger any bug present. The two IC's are what create the oscillating tone. The IC1 operates at .8 Hz where the IC2 runs at about 10
Hz. Frequency is determined by this formula:

$f=1.44/(R1+2R2)C)$

f measured in Hertz, R in megohms, and C in microfarads

The oscillation can be varied by the voltage placed upon pin #5. This is how we create the wave sound. When voltage goes up, so does the frequency, and vice-versa.

Normally, the output pin 3 is a square wave. Since we need varying wave at pin #5, we need a triangular wave. We get this through integrating the square wave created at pin #3 of IC1. It is acheived by D1, D2, R3, R4 an
d C2.

This varying output is fed into the phone line by transformer T1 which has an 8 ohm winding going to pin #3 of IC2 and the 500 end to a 0.1 microfarad capacitator at the phone line.

Enuf talk..let's get movin!

][][][
Schematic Design
][][][

```
         +9v

 __________________|_________________________________________
|      _|___|_                    _|___|_   |
R1    | 4  8 |    _|<D1__R3__  | 4  8 |  R5
|     |      |  |          ||      | |
+-----+2    3+---+          +-+5    2|--+----+----+

|     |      |  |_>|R2__R4__||      |       |    |
R2    | ic1  |              || ic2  |       R6   D3
|   +-+6     |          ____||     6+-+     |    V
|   ||       |          |     |     ||     |    -
+---+-+7     |          |  +--+3    7+-+-----+----+
|     |____1___|          |  |  |____1___|       |
|        |            | |     |         C4
|        |            | |     |         ^
C1        |            C2  T1    _|_._C3|(_. |
^        |           ^ 8--500<_|_.       |
|_____
______|________________|___|_______|____________|
         |
        -G-
```

][][][
Parts List
][][][

C1	10-uF electrolytic capacitator 25 WDVC
C2	300-uF electrolytic capacitator 25 WDVC
C3	0.1-uF capacitator
C4	0.068-uF capacitator
D1-D3	1N914
IC1,IC2	555 timers
R1, R4-R6	1-kilohm resistors
R2	91-kilohm resistor
R3	22 kilohm resistor
T1	500-to-8 ohm audio output transformer

][][][
Construction

When building this unit, it is very useful to use a breadboard or vector board.
I suggest that leads being connected to phone line (T1, C3) end in a jack or a modular connector to make the hookup easier. To test it, hook it to the phone line (not the suspected line) and call the line you suspect is being bugged.
The party you are calling should not answer the phone. Now, the unit is activated. 3 times, every 4 seconds, the oscillator will go up to 10 kHz and back down again..like a bell curve..If there is a frequency sensitive bug on the line, the phone will stop ringing, and you will be able to hear everything said in the room. If the phone keeps ringing, chances are that all is fine..unless the bug requires a multi-frequency trigger..but these are very rare..

So, we can see that 415-BUG-1111 really does work! It creates the tone..any click heard is the Phone Co's (or whoever is bugging) speaker/tape recorder picking up!

[] Bugging I []
[] A Little Electronics Goes A Long, Long, Way []

Purchasing, Planting, Using, Enjoying

NOTE

The recording of any private conversation is against the law unless both parties have given consent, and know that a type of listening/recording device is being used.

WHERE TO GET THEM

As far as bugs goes, don't worry about not being able to obtain them. Sure, there are some suppliers around that only sell to 'Law Enforcement Agencies' only, but most will sell to you, so there is no reason to bother with social engineering yourself one. Anyway, most suppliers that will only sell to law enforcement agencies usually have their products so marked up, its unrealistic. Good bargains, and very high quality equipment can be found offered by a Japanese company called CONY. Usually their products are so reasonable that it makes the competators cry in shame. I suggest you write to them.

CONY MFG CORP
Rm 301 Hirooka Bldg
No 59, 2 Chome
Kangetsu cho
Chikusa ku Nagoya
464 JAPAN

Smile at will...

WHERE AND HOW TO STICK THEM

Assuming you obtain a bug, or any combination of different types of bugs, you will want to use them, for any number of particular purposes. The safest and easiest way to plant a bug is to send the person that you want to know better a nice gift with you know what hidden inside it. Something that they could, say, place on their desk, or display prominently in their place or work or residence. Wrap it nice, and include a small card, and do whatever you feel is appropriate.

They will never guess...

A more dangerous method is to actually obtain entry into the office or residence of the person that you want to know better. If you have success in getting in, planting it, and getting out unnoticed, then you will be safe. Once a bug is planted, you will leave it there even after it becomes inoperative, because, if you have placed considerable risk on yourself to plant it, you do not want to go through that risk again just to retrieve it. Just forget about it. It won't miss you.

There are a number of p
laces to hide your electronic friend:

- o Carefully [!] unscrew a wall socket. There, you will notice some extra, unused space inside. Figure out the rest.

- o Do like the shows on TV. Hide them under a table, or chair. Let your imagination run wild [use good judgement]. You are relitively free, due to today's bug technology, and the short antennaes. Pick an area that is not subject to 'search or routine cleaning'.

- o Dress up like a workman and show up at their house. Make up a good excuse. Gain access. Plant it.

UTILIZATION

You will want to record all that you can get with this bug for later review. Also, take into consideration, that you can't be at the receiver 24 hours a day. The setup to use for maxium efficiency is a recorder with a VOX. Therefore, tape waste will be at a bare minimum. That's also good, because you don't want to be at the receiver just to flip tap
es every half hour to 45 minutes. Also, it would be difficult to review these tapes, because you would have to listen to a half hour recording for an actual half hour, and so on. Well, those half hours will add up into hours, into hours, into hours. Not smart. As said, invest in a VOX. This will make it able to have the recorder skip over those quiet times in your target's house.

To save tape you could slow down the recorder with electronics, if you have the electronics. You might not be successful, because it becomes difficult to tell the speech of people from background noise. Please note that not every technique is discussed here. This is a scratch of the surface.

Also...

If you can, use metal tapes [if the recorder has that capability]. If not, use low noise/extended range tapes.

And...

As with most surveillance equipment, be sure that you know what you are doing. This is a game in which you can be charged hundreds of dollars for something that you could do y
ourself with 35 bucks.

Example...

Some companies sell recorders which claim to be able to record 14 hours on a standard cassette. They have simply removed the pulley from the drive shaft of a Panasonic or Sony recorder that costs less than 50 dollars and jacked up the price 300%. Try it yourself, save money.

ADVANCED TECHNOLOGY

There is a nice device called a shotgun mic that allows you to point it at a window and listen in on a conversation in the immedia
te room, because of the
room's sound waves causing the window glass to vibrate. The window must be closed. Since all you have to do is point it and go, well, they become obviously convienent. And fun. Find one. They might cost a little more, but worth it. And the target is not likely to know he is being watched, so he will not be smart enough to enact countermeasures [more on this the next file].

CLOSING

Not everything is discussed here, but there is enoughto get you started with an exciting and profitable new hobby.

MOBILE TRACKING EQUIPMENT or "Bumper Beepers"an

You remember the little "bug" installed on the bad guys car in the James Bond flicks that allowed Bond to follow the car from a distance? Well this file is a tutorial on them.

First, they do exist, I've built my own, but even the best commercial units intended for law enforcement purposes wont do what the Bond model purports to do, that is, give a printout on a moving map showing the route driven by the bug toter.

The basics of the unit are the transmitter, which is about the size of a pack of cigarettes and is held on via a magnet. And a receiver, using 2 identical antennas, coupled to a center zero meter which gives a heading towards the transmitter. More on these later.

The receiver/display unit is used by pilots, amateur radio operators, and law enforcement and security personnel to track the movements of the transmitter
usually at short ranges, the civil air patrol uses these units to find downed aircraft by tracking the emergency beacon, activated by the impact of the crash. Amateurs play "hunt the fox" to keep illegal transmitters out of the ham bands. Law enforcement personnel track the movement of people, drugs, and weapons by attaching a transmitter to the object (or suspect's car) to be followed.

The transmitter is usually a small VHF or UHF battery operated package dangling a 19" flexible antenna (about the thickness of piano wire). The transmitter does not "beep" per say, but transmits a continual carrier.

The FBI uses 167.xxx mhz for theirs and the local DA uses the intercounty police freq of 155.37. I have seen military models that use 149.xxx mhz around here (air force).

Now the receiver:
Two identical antennas mounted on the chase vehicle (usually magnetic mounts) feed a pair of PIN diodes that feed a phase detector which samples the receiver's IF output. When the received signal is directly in front of you, signals arrive at exactly the same time at each antenna. This is calibrated to read center 0 on the meter. (Incidentally the unit can't tell if the signal is in front or in back of you, so the need to make sure you follow the subject reasonably closely is apparent). If the bug travels say to 10 o'clock on the compass rose, the needle will swing to 4 o'clock on the meter. The object here is to always drive towards zero and you follow the bug in the most direct direction. With a little practice,you can follow a subject on an adjcent street without loosing him.
The meter swings because the signal arrives later at one antenna than the other, causing a voltage change in the phase detector (an Exar Radio-teletype decoder chip in my model).

Some recent units ive seen have Light emitting diodes in a 360 degree circle and use 4 antennas. This gives you full circle detection capabilitys as the phase between pairs of antennas is calculated also.

Now, prevention:
The easiest way to detect if you've been planted with one of these little transmitters, is to walk around the car or whatever with a portable frequency counter and check for an alien RF signal. This is also the recommended method to de-bug your home. A small freq counter with 1.2 ghz capabilitys sells for around $100. today. If you do find a transmitter, have fun with it. Stick it on a train heading out of town, a Greyhound bus, or a over the road tractor-trailer rig....my favorite is to stick it on one of their own vehicles and watch them chase themselves....hehehe.

Free Mail!

Want to be able to mail letters for free? No postage required? It is possible to do, but I gotta warn you that it is a form of mail fraud to do it on purpose...so make sure you only do it by accident IF you do it at all...IS THAT CLEAR???

Let's say you want to send a letter to your friend who lives in... Salt Lake City. You, of course, live in Chicago. Here is how you address the envelope...

```
______________________________________________________________________
|                                   {note lack   |
| Your Friend                            of postage  |
| 666 State Street                        stamp!}    |
| SLC, UT 84444                                  |
|                                           |
|                                           |
|                  Your Name           |
|                  69 Halstead St      |
|                  Chi-Town, IL 60000     |
|                                 |
|                                 |
----------------------------------------------------------------------------
```

Pretty simple eh? Obviously you should use the accurate (real) addresses where indicated (no shit!). What happens when you mail this letter is the post office will mark it RETURN TO SENDER INSUFFICIENT POSTAGE. The sender, as indicated on the envelope, is your friend. Therefore good old Uncle Sam delivers it to the destination you sought. All for free!

Why it works: The Postal Department regulation prohibit delivery of mail that does not have the proper postage. They must return it to the sender for first class letters. Now it may seem a little funny to see a letter that is supposed to be from Salt Lake in a Chicago mail box, but the postal workers probably won't notice and even if they do they can only assume that the letter is correct as addressed...they simply can't spend their time second guessing destinations. Because if they are wrong (and assumed it was mailed from Chicago and sent it thru the system to you on Halstead) they would be breaking their own rules by delivering non-stamped mail *as addressed*. The postal worker, even if he has time to notice or cares, simply must take the envelope at face value and follow regulations. Hence, it gets delivered to your friend.

Glitches: Of the dozens of letters I know have been sent like this once in a while one will come back to you. With all the mail the post office handles some are bound to get thru the system and actually get delivered. It happens. Once I heard of the envelope coming thru with a postage due attachment. This should not happen normally. Post Office regulations say that postage due can only be done when the postage affixed is not enough to cover the cost. It can not be done when there is no postage at all. But again, sometimes it happens. Because of the potential glitch problem don't send important stuff this way. It may boomerang back to you or it may get caught up in the gears of post office red tape and just vanish. It is possible.

Hints: Make the "return" address very complete and legible. Don't indicate in your letter inside or on the back flap that it may have been done on purpose (ie: I hope you get this letter...pretty cool the way I mailed it!). On the evelope will tip off an alert employee, inside could be discovered by a nosey mailman (don't kid yourself...they do read letters once in a while, but they just toss them away when done. I know a mailman who admitted it. This is how many letters get "lost") Also, it won't work for postcards. Make sure the envelope doesn't say address correction requested, or do not forward, or 2nd class mail...or anything else unusual. Just make it looklike your average law abiding letter mailed w/out postage by accident.

Disclaimer/Statement of Facts: Mail Fraud is a big fucking crime. I don't use this technique (I just know of it), I don't suggest you do it either (but it's your choice). Reading, having, telling, and knowing this techinique is NOT against the law...neither is distributing it.

IF you decide to try it the odds are %99.99999999999999999 percent that no one will ever know. But as a precaution NEVER admit, brag, tell anyone that you EVER mailed a letter w/out postage ON PURPOSE. We all make mistakes...even Ronny Raygun. Remember, the only scumbag that came out of Watergate with both his testicles was G. Gordon Liddy and he KEPT HIS MOUTH SHUT. Learn by his example.

But hey! I don't mean to get preachy. Have fun with this. Sleep easier now that the potential exists to mail free. Rebels unite, you have nothing to loose but your inhibitions.

PPS: I didn't originate this postage free system, someone told me about it many years ago. It is probably quite common but many I have talked to have not heard it so I thought I'd type it up and distribute. If you found yourself thinking..."how old" than you are right. If you found yourself thinking "how stupid" then go fuck yourself. Knowledge is power and must be distributed or we will all perish in a bourgeoise nuclear death.

Part Two: Networks
~~~~~~~~~~~~~~~~~~

The best place to begin hacking (other than a college) is on one of the bigger networks such as Telenet. Why? First, there is a wide variety of computers to choose from, from small Micro-Vaxen to huge Crays. Second, the networks are fairly well documented. It's easier to find someone who can help you with a problem off of Telenet than it is to find assistance concerning your local college computer or high school machine. Third, the networks are safer. Because of the enormous number of calls that are fielded every day by the big networks, it is not financially practical to keep track of where every call and connection are made from. It is also very easy to disguise your location using the network, which makes your hobby much more secure.

Telenet has more computers hooked to it than any other system in the world once you consider that from Telenet you have access to Tymnet, ItaPAC, JANET, DATAPAC, SBDN, PandaNet, THEnet, and a whole host of other networks, all of which you can connect to from your terminal.

The first step that you need to take is to identify your local dialup port. This is done by dialing 1-800-424-9494 (1200 7E1) and connecting. It will spout some garbage at you and then you'll get a prompt saying 'TERMINAL='. This is your terminal type. If you have vt100 emulation, type it in now. Or just hit return and it will default to dumb terminal mode.

You'll now get a prompt that looks like a @. From here, type @c mail <cr> and then it will ask for a Username. Enter 'phones' for the username. When it asks for a password, enter 'phones' again. From this point, it is menu driven. Use this to locate your local dialup, and call it back locally. If you don't have a local dialup, then use whatever means you wish to connect to one long distance (more on this later.)

When you call your local dialup, you will once again go through the TERMINAL= stuff, and once again you'll be presented with a @. This prompt lets you know you are connected to a Telenet PAD. PAD stands for either Packet Assembler/Disassembler (if you talk to an engineer), or Public Access Device
~~~~~~~~~~~~~~~~~~

(if you talk to Telenet's marketing people.) The first description is more correct.

Telenet works by taking the data you enter in on the PAD you dialed into, bundling it into a 128 byte chunk (normally... this can be changed), and then transmitting it at speeds ranging from 9600 to 19,200 baud to another PAD, who then takes the data and hands it down to whatever computer or system it's connected to. Basically, the PAD allows two computers that have different baud rates or communication protocols to communicate with each other over a long distance. Sometimes you'll notice a time lag in the remote machines response. This is called PAD Delay, and is to be expected when you're sending data through several different links.

What do you do with this PAD? You use it to connect to remote computer systems by typing 'C' for connect and then the Network User Address (NUA) of the system you want to go to.

```
   An NUA takes the form of   031103130002520
                             \___/\___/\___/
                               |    |    |
                               |    |    |____ network address
                               |    |__________ area prefix
                               |_______________ DNIC
```

This is a summary of DNIC's (taken from Blade Runner's file on ItaPAC) according to their country and network name.

DNIC	Network Name	Country	DNIC	Network Name	Country
02041	Datanet 1	Netherlands	03110	Telenet	USA
02062	DCS	Belgium	03340	Telepac	Mexico
02080	Transpac	France	03400	UDTS-Curacau	Curacau
02284	Telepac	Switzerland	04251	Isranet	Israel
02322	Datex-P	Austria	04401	DDX-P	Japan
02329	Radaus	Austria	04408	Venus-P	Japan
02342	PSS	UK	04501	Dacom-Net	South Korea
02382	Datapak	Denmark	04542	Intelpak	Singapore
02402	Datapak	Sweden	05052	Austpac	Australia
02405	Telepak	Sweden	05053	Midas	Australia
02442	Finpak	Finland	05252	Telepac	Hong Kong
02624	Datex-P	West Germany	05301	Pacnet	New Zealand
02704	Luxpac	Luxembourg	06550	Saponet	South Africa
02724	Eirpak	Ireland	07240	Interdata	Brazil
03020	Datapac	Canada	07241	Renpac	Brazil
03028	Infogram	Canada	09000	Dialnet	USA
03103	ITT/UDTS	USA	07421	Dompac	French Guiana
03106	Tymnet	USA			

There are two ways to find interesting addresses to connect to. The first and easiest way is to obtain a copy of the LOD/H Telenet Directory from the LOD/H Technical Journal #4 or 2600 Magazine. Jester Sluggo also put out a good list of non-US addresses in Phrack Inc. Newsletter Issue 21. These files will tell you the NUA, whether it will accept collect calls or not, what type of computer system it is (if known) and who it belongs to (also if known.)

The second method of locating interesting addresses is to scan for them manually. On Telenet, you do not have to enter the 03110 DNIC to connect to a Telenet host. So if you saw that 031104120006140 had a VAX on it you wanted to look at, you could type @c 412 614 (0's can be ignored most of the time.)

If this node allows collect billed connections, it will say 412 614 CONNECTED and then you'll possibly get an identifying header or just a Username: prompt. If it doesn't allow collect connections, it will give you a message such as 412 614 REFUSED COLLECT CONNECTION with some error codes out to the right, and return you to the @ prompt.

There are two primary ways to get around the REFUSED COLLECT message. The first is to use a Network User Id (NUI) to connect. An NUI is a username/pw combination that acts like a charge account on Telenet. To collect to node 412 614 with NUI junk4248, password 525332, I'd type the following:
@c 412 614,junk4248,525332 <---- the 525332 will *not* be echoed to the screen. The problem with NUI's is that they're hard to come by unless you're a good social engineer with a thorough knowledge of Telenet (in which case you probably aren't reading this section), or you have someone who can provide you with them.

The second way to connect is to use a private PAD, either through an X.25 PAD or through something like Netlink off of a Prime computer (more on these two below.)

The prefix in a Telenet NUA oftentimes (not always) refers to the phone Area Code that the computer is located in (i.e. 713 xxx would be a computer in Houston, Texas.) If there's a particular area you're interested in, (say, New York City 914), you could begin by typing @c 914 001 <cr>. If it connects, you make a note of it and go on to 914 002. You do this until you've found some interesting systems to play with.

Not all systems are on a simple xxx yyy address. Some go out to four or five digits (914 2354), and some have decimal or numeric extensions (422 121A = 422 121.01). You have to play with them, and you never know what you're going to find. To fully scan out a prefix would take ten million attempts per prefix. For example, if I want to scan 512 completely, I'd have to start with 512 00000.00 and go through 512 00000.99, then increment the address by 1 and try 512 00001.00 through 512 00001.99. A lot of scanning. There are plenty of neat computers to play with in a 3-digit scan, however, so don't go berserk with the extensions.

Sometimes you'll attempt to connect and it will just be sitting there after one or two minutes. In this case, you want to abort the connect attempt by sending a hard break (this varies with different term programs, on Procomm, it's ALT-B), and then when you get the @ prompt back, type 'D' for disconnect.

If you connect to a computer and wish to disconnect, you can type <cr> @ <cr> and you it should say TELENET and then give you the @ prompt. From there, type D to disconnect or CONT to re-connect and continue your session uninterrupted.

Outdials, Network Servers, and PADs
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

In addition to computers, an NUA may connect you to several other things. One of the most useful is the outdial. An outdial is nothing more than a modem you can get to over telenet- similar to the PC Pursuit concept, except that these don't have passwords on them most of the time.

When you connect, you will get a message like 'Hayes 1200 baud outdial, Detroit, MI', or 'VEN-TEL 212 Modem', or possibly 'Session 1234 established on Modem 5588'. The best way to figure out the commands on these is to type ? or H or HELP- this will get you all the information that you need to use one.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Safety tip here- when you are hacking *any* system through a phone dialup, always use an outdial or a diverter, especially if it is a local phone number to you. More people get popped hacking on local computers than you can imagine, Intra-LATA calls are the easiest things in the world to trace inexpensively.

Another nice trick you can do with an outdial is use the redial or macro function that many of them have. First thing you do when you connect is to invoke the 'Redial Last Number' facility. This will dial the last number used, which will be the one the person using it before you typed. Write down the number, as no one would be calling a number without a computer on it. This is a good way to find new systems to hack. Also, on a VENTEL modem, type 'D' for Display and it will display the five numbers stored as macros in the modem's memory.

There are also different types of servers for remote Local Area Networks (LAN) that have many machine all over the office or the nation connected to them. I'll discuss identifying these later in the computer ID section.

And finally, you may connect to something that says 'X.25 Communication PAD' and then some more stuff, followed by a new @ prompt. This is a PAD just like the one you are on, except that all attempted connections are billed to the PAD, allowing you to connect to those nodes who earlier refused collect connections.

This also has the added bonus of confusing where you are connecting from. When a packet is transmitted from PAD to PAD, it contains a header that has the location you're calling from. For instance, when you first connected to Telenet, it might have said 212 44A CONNECTED if you called from the 212 area code. This means you were calling PAD number 44A in the 212 area. That 21244A will be sent out in the header of all packets leaving the PAD.

Once you connect to a private PAD, however, all the packets going out from *it* will have it's address on them, not yours. This can be a valuable buffer between yourself and detection.

Phone Scanning
~~~~~~~~~~~~~~

Finally, there's the time-honored method of computer hunting that was made famous among the non-hacker crowd by that Oh-So-Technically-Accurate movie Wargames. You pick a three digit phone prefix in your area and dial every number from 0000 --> 9999 in that prefix, making a note of all the carriers you find. There is software available to do this for nearly every computer in the world, so you don't have to do it by hand.

Part Three: I've Found a Computer, Now What?
~~~~~~

This next section is applicable universally. It doesn't matter how you found this computer, it could be through a network, or it could be from carrier scanning your High School's phone prefix, you've got this prompt this prompt, what the hell is it?

I'm *NOT* going to attempt to tell you what to do once you're inside of any of these operating systems. Each one is worth several G-files in its own right. I'm going to tell you how to identify and recognize certain OpSystems, how to approach hacking into them, and how to deal with something that you've never seen before and have know idea what it is.

VMS- The VAX computer is made by Digital Equipment Corporation (DEC), and runs the VMS (Virtual Memory System) operating system. VMS is characterized by the 'Username:' prompt. It will not tell you if you've entered a valid username or not, and will disconnect you after three bad login attempts. It also keeps track of all failed login attempts and informs the owner of the account next time s/he logs in how many bad login attempts were made on the account. It is one of the most secure operating systems around from the outside, but once you're in there are many things that you can do to circumvent system security. The VAX also has the best set of help files in the world. Just type HELP and read to your heart's content.

Common Accounts/Defaults: [username: password [[,password]]]

SYSTEM:	OPERATOR or MANAGER or SYSTEM or SYSLIB
OPERATOR:	OPERATOR
SYSTEST:	UETP
SYSMAINT:	SYSMAINT or SERVICE or DIGITAL
FIELD:	FIELD or SERVICE
GUEST:	GUEST or unpassworded
DEMO:	DEMO or unpassworded
DECNET:	DECNET

DEC-10- An earlier line of DEC computer equipment, running the TOPS-10 operating system. These machines are recognized by their '.' prompt. The DEC-10/20 series are remarkably hacker-friendly, allowing you to enter several important commands without ever logging into the system. Accounts are in the format [xxx,yyy] where xxx and yyy are integers. You can get a listing of the accounts and the process names of everyone on the system before logging in with the command .systat (for SYstem STATus). If you seen an account that reads [234,1001] BOB JONES, it might be wise to try BOB or JONES or both for a password on this account. To login, you type .login xxx,yyy and then type the password when prompted for it. The system will allow you unlimited tries at an account, and does not keep records of bad login attempts. It will also inform you if the UIC you're trying (UIC = User Identification Code, 1,2 for example) is bad.

Common Accounts/Defaults:

1,2:	SYSLIB or OPERATOR or MANAGER
2,7:	MAINTAIN
5,30:	GAMES

UNIX- There are dozens of different machines out there that run UNIX. While some might argue it isn't the best operating system in the world, it is certainly the most widely used. A UNIX system will usually have a prompt like 'login:' in lower case. UNIX also will give you unlimited shots at logging in (in most cases), and there is usually no log kept of bad attempts.

Common Accounts/Defaults: (note that some systems are case sensitive, so use lower case as a general rule. Also, many times the accounts will be unpassworded, you'll just drop right in!)

root:	root
admin:	admin

sysadmin:	sysadmin or admin
unix:	unix
uucp:	uucp
rje:	rje
guest:	guest
demo:	demo
daemon:	daemon
sysbin:	sysbin

Prime- Prime computer company's mainframe running the Primos operating system. The are easy to spot, as the greet you with 'Primecon 18.23.05' or the like, depending on the version of the operating system you run into. There will usually be no prompt offered, it will just look like it's sitting there. At this point, type 'login <username>'. If it is a pre-18.00.00 version of Primos, you can hit a bunch of ^C's for the password and you'll drop in. Unfortunately, most people are running versions 19+. Primos also comes with a good set of help files. One of the most useful features of a Prime on Telenet is a facility called NETLINK. Once you're inside, type NETLINK and follow the help files. This allows you to connect to NUA's all over the world using the 'nc' command. For example, to connect to NUA 026245890040004, you would type @nc :26245890040004 at the netlink prompt.

Common Accounts/Defaults:

PRIME	PRIME or PRIMOS
PRIMOS_CS	PRIME or PRIMOS
PRIMENET	PRIMENET
SYSTEM	SYSTEM or PRIME
NETLINK	NETLINK
TEST	TEST
GUEST	GUEST
GUEST1	GUEST

HP-x000- This system is made by Hewlett-Packard. It is characterized by the ':' prompt. The HP has one of the more complicated login sequences around- you type 'HELLO SESSION NAME,USERNAME,ACCOUNTNAME,GROUP'. Fortunately, some of these fields can be left blank in many cases. Since any and all of these fields can be passworded, this is not the easiest system to get into, except for the fact that there are usually some unpassworded accounts around. In general, if the defaults don't work, you'll have to brute force it using the common password list (see below.) The HP-x000 runs the MPE operating system, the prompt for it will be a ':', just like the logon prompt.

Common Accounts/Defaults:

MGR.TELESUP,PUB	User: MGR Acct: HPONLY Grp: PUB
MGR.HPOFFICE,PUB	unpassworded
MANAGER.ITF3000,PUB	unpassworded
FIELD.SUPPORT,PUB	user: FLD, others unpassworded
MAIL.TELESUP,PUB	user: MAIL, others unpassworded
MGR.RJE	unpassworded
FIELD.HPPl89 ,HPPl87,HPPl89,HPPl96	unpassworded
MGR.TELESUP,PUB,HPONLY,HP3	unpassworded

IRIS- IRIS stands for Interactive Real Time Information System. It originally ran on PDP-11's, but now runs on many other minis. You can spot an IRIS by the 'Welcome to "IRIS" R9.1.4 Timesharing' banner, and the ACCOUNT ID? prompt. IRIS allows unlimited tries at hacking in, and keeps no logs of bad attempts. I don't know any default passwords, so just try the common ones from the password database below.

Common Accounts:

MANAGER
BOSS
SOFTWARE
DEMO
PDP8
PDP11
ACCOUNTING

VM/CMS- The VM/CMS operating system runs in International Business Machines (IBM) mainframes. When you connect to one of these, you will get message similar to 'VM/370 ONLINE', and then give you a '.' prompt, just like TOPS-10 does. To login, you type 'LOGON <username>'.

Common Accounts/Defaults are:

AUTOLOG1:	AUTOLOG or AUTOLOG1
CMS:	CMS
CMSBATCH:	CMS or CMSBATCH
EREP:	EREP
MAINT:	MAINT or MAINTAIN
OPERATNS:	OPERATNS or OPERATOR
OPERATOR:	OPERATOR
RSCS:	RSCS
SMART:	SMART
SNA:	SNA
VMTEST:	VMTEST
VMUTIL:	VMUTIL
VTAM:	VTAM

NOS- NOS stands for Networking Operating System, and runs on the Cyber computer made by Control Data Corporation. NOS identifies itself quite readily, with a banner of 'WELCOME TO THE NOS SOFTWARE SYSTEM. COPYRIGHT CONTROL DATA 1978,1987'. The first prompt you will get will be FAMILY:. Just hit return here. Then you'll get a USER NAME: prompt. Usernames are typically 7 alpha-numerics characters long, and are *extremely* site dependent. Operator accounts begin with a digit, such as 7ETPDOC.

Common Accounts/Defaults:

$SYSTEM	unknown
SYSTEMV	unknown

Decserver- This is not truly a computer system, but is a network server that has many different machines available from it. A Decserver will say 'Enter Username>' when you first connect. This can be anything, it doesn't matter, it's just an identifier. Type 'c', as this is the least conspicuous thing to enter. It will then present you with a 'Local>' prompt. From here, you type 'c <systemname>' to connect to a system. To get a list of system names, type 'sh services' or 'sh nodes'. If you have any problems, online help is available with the 'help' command. Be sure and look for services named 'MODEM' or 'DIAL' or something similar, these are often outdial modems and can be useful!

GS/1- Another type of network server. Unlike a Decserver, you can't predict what prompt a GS/1 gateway is going to give you. The default prompt it 'GS/1>', but this is redifinable by the system administrator. To test for a GS/1, do a 'sh d'. If that prints out a large list of defaults (terminal speed, prompt, parity, etc...), you are on a GS/1. You connect in the same manner as a Decserver, typing 'c <systemname>'. To find out what systems are available, do a 'sh n' or a 'sh c'. Another trick is to do a 'sh m', which will sometimes show you a list of macros for logging onto a system. If there is a macro named VAX, for instance, type 'do VAX'.

The above are the main system types in use today. There are hundreds of minor variants on the above, but this should be enough to get you started.

Unresponsive Systems
~~~~~~~~~~~~~~~~~~~~~~

Occasionally you will connect to a system that will do nothing but sit there. This is a frustrating feeling, but a methodical approach to the system will yield a response if you take your time. The following list will usually make *something* happen.

1) Change your parity, data length, and stop bits. A system that won't respond at 8N1 may react at 7E1 or 8E2 or 7S2. If you don't have a term program that will let you set parity to EVEN, ODD, SPACE, MARK, and NONE, with data length of 7 or 8, and 1 or 2 stop bits, go out and buy one. While having a good term program isn't absolutely necessary, it sure is helpful.
2) Change baud rates. Again, if your term program will let you choose odd baud rates such as 600 or 1100, you will occasionally be able to penetrate some very interesting systems, as most systems that depend on a strange baud rate seem to think that this is all the security they need...
3) Send a series of <cr>'s.
4) Send a hard break followed by a <cr>.
5) Type a series of .'s (periods). The Canadian network Datapac responds to this.
6) If you're getting garbage, hit an 'i'. Tymnet responds to this, as does a MultiLink II.
7) Begin sending control characters, starting with ^A --> ^Z.
8) Change terminal emulations. What your vt100 emulation thinks is garbage may all of a sudden become crystal clear using ADM-5 emulation. This also relates to how good your term program is.
9) Type LOGIN, HELLO, LOG, ATTACH, CONNECT, START, RUN, BEGIN, LOGON, GO, JOIN, HELP, and anything else you can think of.
10) If it's a dialin, call the numbers around it and see if a company answers. If they do, try some social engineering.

Brute Force Hacking
~~~~~~~~~~~~~~~~~~~~~

There will also be many occasions when the default passwords will not work on an account. At this point, you can either go onto the next system on your list, or you can try to 'brute-force' your way in by trying a large database of passwords on that one account. Be careful, though! This works fine on systems that don't keep track of invalid logins, but on a system like a VMS, someone is going to have a heart attack if they come back and see '600 Bad Login Attempts Since Last Session' on their account. There are also some operating systems that disconnect after 'x' number of invalid login attempts and refuse to allow any more attempts for one hour, or ten minutes, or sometimes until the next day.

The following list is taken from my own password database plus the database of passwords that was used in the Internet UNIX Worm that was running around in November of 1988. For a shorter group, try first names, computer terms, and obvious things like 'secret', 'password', 'open', and the name of the account. Also try the name of the company that owns the computer system (if known), the company initials, and things relating to the products the company makes or deals with.

Password List
=============

aaa
academia
ada
adrian
aerobics
airplane
albany
albatross
albert
alex
alexander
algebra
alias
alpha
alphabet
ama
amy
analog
anchor
andy
andrea
animal
answer
anything
arrow
arthur
asshole
athena
atmosphere
bacchus
badass
bailey
banana
bandit
banks

daniel
danny
dave
deb
debbie
deborah
december
desperate
develop
diet
digital
discovery
disney
dog
drought
duncan
easy
eatme
edges
edwin
egghead
eileen
einstein
elephant
elizabeth
ellen
emerald
engine
engineer
enterprise
enzyme
euclid
evelyn
extension
fairway

jester
johnny
joseph
joshua
judith
juggle
julia
kathleen
kermit
kernel
knight
lambda
larry
lazarus
lee
leroy
lewis
light
lisa
louis
lynne
mac
macintosh
mack
maggot
magic
malcolm
mark
markus
marty
marvin
master
maurice
merlin
mets

rascal
really
rebecca
remote
rick
reagan
robot
robotics
rolex
ronald
rosebud
rosemary
roses
ruben
rules
ruth
sal
saxon
scheme
scott
scotty
secret
sensor
serenity
sex
shark
sharon
shit
shiva
shuttle
simon
simple
singer
single
smile

bass
batman
beauty
beaver
beethoven
beloved
benz
beowulf
berkeley
berlin
beta
beverly
bob
brenda
brian
bridget
broadway
bumbling
cardinal
carmen
carolina
caroline
castle
cat
celtics
change
charles
charming
charon
chester
cigar
classic
coffee
coke
collins
comrade
computer
condo
condom
cookie
cooper
create
creation
creator
cretin
daemon
dancer

felicia
fender
fermat
finite
flower
foolproof
football
format
forsythe
fourier
fred
friend
frighten
fun
gabriel
garfield
gauss
george
gertrude
gibson
ginger
gnu
golf
golfer
gorgeous
graham
gryphon
guest
guitar
hacker
harmony
harold
harvey
heinlein
hello
help
herbert
honey
horse
imperial
include
ingres
innocuous
irishman
isis
japan
jessica

michael
michelle
mike
minimum
minsky
mogul
moose
mozart
nancy
napoleon
network
newton
next
olivia
oracle
orca
orwell
osiris
outlaw
oxford
pacific
painless
pam
paper
password
pat
patricia
penguin
pete
peter
philip
phoenix
pierre
pizza
plover
polynomial
praise
prelude
prince
protect
pumpkin
puppet
rabbit
rachmaninoff
rainbow
raindrop
random

smiles
smooch
smother
snatch
snoopy
soap
socrates
spit
spring
subway
success
summer
super
support
surfer
suzanne
tangerine
tape
target
taylor
telephone
temptation
tiger
toggle
tomato
toyota
trivial
unhappy
unicorn
unknown
urchin
utility
vicky
virginia
warren
water
weenie
whatnot
whitney
will
william
willie
winston
wizard
wombat
yosemite
zap

Part Four: Wrapping it up!

~~~~~~~~~~~~~~~~~~~~~~~~~~~

References:
~~~~~~~~~~~~~~~~~~~~~~~~~~~

1) Introduction to ItaPAC by Blade Runner
   Telecom Security Bulletin #1
2) The IBM VM/CMS Operating System by Lex Luthor
   The LOD/H Technical Journal #2
3) Hacking the IRIS Operating System by The Leftist
   The LOD/H Technical Journal #3
4) Hacking CDC's Cyber by Phrozen Ghost
   Phrack Inc. Newsletter #18
5) USENET comp.risks digest (various authors, various issues)
6) USENET unix.wizards forum (various authors)
7) USENET info-vax forum (various authors)

Recommended Reading:
1) Hackers by Steven Levy
2) Out of the Inner Circle by Bill Landreth
3) Turing's Man by J. David Bolter
4) Soul of a New Machine by Tracy Kidder
5) Neuromancer, Count Zero, Mona Lisa Overdrive, and Burning Chrome, all
   by William Gibson
6) Reality Hackers Magazine c/o High Frontiers, P.O. Box 40271, Berkeley,
   California, 94704, 415-995-2606
7) Any of the Phrack Inc. Newsletters & LOD/H Technical Journals you can find.

Acknowledgements:
Thanks to my wife for putting up with me.
Thanks to Lone Wolf for the RSTS & TOPS assistance.
Thanks to Android Pope for proofreading, suggestions, and beer.
Thanks to The Urvile/Necron 99 for proofreading & Cyber info.
Thanks to Eric Bloodaxe for wading through all the trash.
Thanks to the users of Phoenix Project for their contributions.
Thanks to Altos Computer Systems, Munich, for the chat system.
Thanks to the various security personel who were willing to talk to
me about how they operate.

Counterfeiting Money

Before reading this article, it would be a very good idea to get a book on photo offset printing, for this is the method used in counterfeiting US currency. If you are familiar with this method of printing, counterfeiting should be a simple task for you.

Genuine currency is made by a process called "gravure", which involves etching a metal block. Since etching a metal block is impossible to do by hand, photo offset printing comes into the process.

Photo offset printing starts by making negatives of the currency with a camera, and putting the negatives on a piece of masking material (usually orange in color). The stripped negatives, commonly called "flats", are then exposed to a lithographic plate with an arc light plate maker. The burned plates are then developed with the proper developing chemical. One at a time, these plates are wrapped around the plate cylinder of the press.

The press to use should be an 11 by 14 offset, such as the AB Dick 360. Make 2 negatives of the portrait side of the bill, and 1 of the back side. After developing them and letting them dry, take them to a light table. Using opaque on one of the portrait sides, touch out all the green, which is the seal and the serial numbers. The back side does not require any retouching, because it is all one color. Now, make sure all of the negatives are registered (lined up correctly) on the flats. By the way, every time you need another serial number, shoot 1 negative of the portrait side, cut out the serial number, and remove the old serial number from the flat replacing it with the new one.

Now you have all 3 flats, and each represents a different color: black, and 2 shades of green (the two shades of green are created by mixing inks). Now you are ready to burn the plates. Take a lithographic plate and etch three marks on it. These marks must be 2 and 9/16 inches apart, starting on one of the short edges. Do the same thing to 2 more plates. Then, take 1 of the flats and place it on the plate, exactly lining the short edge up with the edge of the plate. Burn it, move it up to the next mark, and cover up the exposed area you have already burned. Burn that, and do the same thing 2 more times, moving the flat up one more mark. Do the same process with the other 2 flats (each on a separate plate). Develop all three plates. You should now have 4 images on each plate with an equal space between each bill.

The paper you will need will not match exactly, but it will do for most situations. The paper to use should have a 25% rag content. By the way, Disaperf computer paper (invisible perforation) does the job well. Take the paper and load it into the press. Be sure to set the air, buckle, and paper thickness right. Start with the black plate (the plate without the serial numbers). Wrap it around the cylinder and load black ink in. Make sure you run more than you need because there will be a lot of rejects. Then, while that is printing, mix the inks for the serial numbers and the back side. You will need to add some white and maybe yellow to the serial number ink. You also need to add black to the back side. Experiment until you get it right. Now, clean the press and print the other side. You will now have a bill with no green seal or serial numbers. Print a few with one serial number, make another and repeat. Keep doing this until you have as many different numbers as you want. Then cut the bills to the exact size with a paper cutter. You should have printed a large amount of money by now, but there is still one problem; the paper is pure white. To dye it, mix the following in a pan: 2 cups of hot water, 4 tea bags, and about 16 to 20 drops of green food coloring (experiment with this). Dip one of the bills in and compare it to a genuine US bill. Make the necessary adjustments, and dye all the bills. Also, it is a good idea to make them look used. For example, wrinkle them, rub coffee grinds on them, etc.

As before mentioned, unless you are familiar with photo offset printing, most of the information in this article will be fairly hard to understand. Along with getting a book on photo offset printing, try to see the movie "To Live and Die in LA". It is about a counterfeiter, and the producer does a pretty good job of showing how to counterfeit. A good book on the subject is "The Poor Man's James Bond".

If all of this seems too complicated to you, there is one other method available for counterfeiting: The Canon color laser copier. The Canon can replicate ANYTHING in vibrant color, including US currency. But, once again, the main problem in counterfeiting is the paper used. So, experiment, and good luck!

Credit Card Fraud

For most of you out there, money is hard to come by. Until now:

With the recent advent of plastic money (credit cards), it is easy to use someone else's credit card to order the items you have always desired in life. The stakes are high, but the payoff is worth it.

Step One: Getting the credit card information

First off, you must obtain the crucial item: someone's credit card number. The best way to get credit card numbers is to take the blue carbons used in a credit card transaction at your local department store. These can usually be found in the garbage can next to the register, or for the more daring, in the garbage dumpster behind the store. But, due to the large amount of credit card fraud, many stores have opted to use a carbonless transaction sheet, making things much more difficult. This is where your phone comes in handy.

First, look up someone in the phone book, and obtain as much information as possible about them. Then, during business hours, call in a very convincing voice - "Hello, this is John Doe from the Visa Credit Card Fraud Investigations Department. We have been informed that your credit card may have been used for fraudulent purposes, so will you please read off the numbers appearing on your Visa card for verification." Of course, use your imagination! Believe it or not, many people will fall for this ploy and give out their credit information.

Now, assuming that you have your victim's credit card number, you should be able to decipher the information given.

Step Two: Recognizing information from carbon copies

Card examples:

[American Express]

XXXX XXXXXX XXXXX
MM/Y1 THRU MM/Y2
JOE SHMOE

[American Express]
XXXX XXXXXX XXXXX
MM/Y1 THRU MM/Y2
JOE SHMOE

Explanation:

MM/Y1 is the date the card was issued, and MM/Y2 is the expiration date. The American Express Gold Card has numbers XXXXXX XXXXXXXX XXXXXXXX, and is covered for up to $5000.00, even if the card holder is broke.

[Mastercard]
5XXX XXXX XXXX XXXX
XXXX AAA DD-MM-YY MM/YY
JOE SHMOE

Explanation:

XXXX in the second row may be asked for during the ordering process. The first date is when the card was new, and the second is when the card expires. The most frequent number combination used is 5424 1800 XXXX XXXX. There are many of these cards in circulation, but many of these are on wanted lists, so check these first.

[Visa]
4XXX XXX(X) XXX(X) XXX(X)
MM/YY   MM/YY*VISA
JOE SHMOE

Explanation:

Visa is the most abundant card, and is accepted almost everywhere. The "*VISA" is sometimes replaced with "BWG", or followed with a special code. These codes are as follows:

[1] MM/YY*VISA V - Preferred Card
[2] MM/YY*VISA CV - Classic Card
[3] MM/YY*VISA PV - Premier Card

Preferred Cards are backed with money, and are much safer to use. Classic Cards are newer, harder to reproduce cards with decent backing. Premier Cards are Classic Cards with Preferred coverage. Common numbers are 4448 020 XXX XXX, 4254 5123 6000 XXXX, and 4254 5123 8500 XXXX. Any 4712 1250 XXXX XXXX cards are IBM Credit Union cards, and are risky to use, although they are usually covered for large purchases.

Step Three: Testing credit

You should now have a Visa, Mastercard, or American Express credit card number, with the victim's address, zip code, and phone number. By the way, if you have problems getting the address, most phone companies offer the Address Tracking Service, which is a special number you call that will give you an address from a phone number, at a nominal charge. Now you need to check the balance of credit on the credit card (to make sure you don't run out of money), and you must also make sure that the card isn't stolen. To do this you must obtain a phone number that businesses use to check out credit cards during purchases. If you go to a department store, watch the cashier when someone makes a credit card purchase. He/she will usually call a phone number, give the credit information, and then give what is called a "Merchant Number". These numbers are usually written down on or around the register. It is easy to either find these numbers and copy them, or to wait until they call one in. Watch what they dial and wait for the 8 digit (usually) merchant number. Once you call the number, in a calm voice, read off the account number, merchant number, amount, and expiration date. The credit bureau will tell you if it is ok, and will give you an authorization number. Pretend you are writing this number down, and repeat it back to them to check it. Ignore this number completely, for it serves no real purpose. However, once you do this, the bank removes dollars equal to what you told them, because the card was supposedly used to make a purchase. Sometimes you can trick the operator by telling her the customer changed his mind and decided not to charge it. Of course, some will not allow this. Remember at all times that you are supposed to be a store clerk calling to check out the card for a purchase. Act like you are talking with a customer when he/she "cancels".

Step Four: The drop

Once the cards are cleared, you must find a place to have the package sent. NEVER use a drop more than once. The following are typical drop sites:

[1] An empty house

An empty house makes an excellent place to send things. Send the package UPS, and leave a note on the door saying, "UPS. I work days, 8 to 6. Could you please leave the package on the back door step?" You can find dozens of houses from a real estate agent by telling them you want to look around for a house. Ask for a list of twenty houses for sale, and tell them you will check out the area. Do so, until you find one that suits your needs.

[2] Rent A Spot

U-Haul sometimes rents spaces where you can have packages sent and signed for. End your space when the package arrives.

[3] People's houses

Find someone you do not know, and have the package sent there. Call ahead saying that "I called the store and they sent the package to the wrong address. It was already sent, but can you keep it there for me?" This is a very reliable way if you keep calm when talking to the people.

Do NOT try post office boxes. Most of the time, UPS will not deliver to a post office box, and many people have been caught in the past attempting to use a post office box. Also, when you have determined a drop site, keep an eye on it for suspicious characters and cars that have not been there before.

Step Five: Making the transaction

You should now have a reliable credit card number with all the necessary billing information, and a good drop site.

The best place to order from is catalogues, and mail order houses. It is in your best interest to place the phone call from a pay phone, especially if it is a 1-800 number. Now, when you call, don't try to disguise your voice, thinking you will trick the salesperson into believing you are an adult. These folks are trained to detect this, so your best bet is to order in your own voice. They will ask for the following: name, name as it appears on card, phone number, billing address, expiration date, method of shipping, and product. Ask if they offer UPS Red shipping (next day arrival), because it gives them less time to research an order. If you are using American Express, you might have a bit of a problem shipping to an address other than the billing address. Also, if the salesperson starts to ask questions, do NOT hang up. Simply talk your way out of the situation, so you won't encourage investigation on the order.

If everything goes right, you should have the product, free of charge. Insurance picks up the tab, and no one is any wiser. Be careful, and try not to order anything over $500. In some states, UPS requires a signature for anything over $200, not to mention that anything over $200 is defined as grand theft, as well as credit fraud. Get caught doing this, and you will bite it for a couple of years. Good luck!

Highway radar jamming

Most drivers wanting to make better time on the open road will invest in one of those expensive radar detectors. However, this device will not work against a gun type radar unit in which the radar signal is not present until the cop has your car in his sights and pulls the trigger. Then it is TOO LATE for you to slow down. A better method is to continuously jam any signal with a radar signal of your own. I have tested this idea with the cooperation of a local cop and found that his unit reads random numbers when my car approached him. It is suprisingly easy to make a low power radar transmitter. A nifty little semiconductor called a Gunn Diode will generate microwaves when supplied with the 5 to 10 volt DC and enclosed in the correct size cavity (resonater). An

8 to 3 terminal regulator can be used to get this voltage from a car's 12v system. However, the correct construction and tuning of the cavity is difficult without good microwave measurement equipment. Police radars commonly operate on the K band at 22 ghz. Or more often on the X band at 10.525 ghz. most microwave intruder alarms and motion detectors (mounted over automatic doors in supermarkets & banks, etc.) contain a Gunn type transmitter/receiver combination that transmits about 10 kilowatts at 10.525 ghz. These units work perfectly as jammers. If you cannot get one locally, write to Microwave Associates in Burlington, Massachusettes and ask them for info on 'Gunnplexers' for ham radio use. When you get the unit it may be mounted in a plastic box on the dash or in a weather-proff enclosure behind the PLASTIC grille. Switch on the power when on an open highway. The unit will not jam radar to the side or behind the car so don't go speeding past the radar trap. An interesting phenomena you will notice is that the drivers who are in front of you who are using detectors will hit their brakes as you approach large metal signs and bridges. Your signal is bouncing off of these objects and triggering their radar detectors!   HAVE FUN!

-Jolly Roger-

P.S. If you are interested in this sort of thing, get a copy of POPULAR COMMUNICATIONS. The ads in there tell you where you can get all kinds of info on all kinds of neat equipment for all kinds of neat things!

Downloaded From P-80 International Information Systems 304-744-2253

The easiest way to hotwire cars

Get in the car. Look under the dash. If it enclosed, forget it unless you want to cut through it. If you do, do it near the ignition. Once you get behind or near the ignition look for two red wires. In older cars red was the standard color, if not, look for two matched pairs. When you find them, cross them and take off!   -

Ripping off Change Machines   by the Jolly Roger

Have you ever seen one of those really big changer machines in airports laundrymats or arcades that dispense change when you put in your 1 or 5 dollar bill? Well then, here is an article for you.

1) Find the type of change machine that you slide in your bill length

wise, not the type where you put the bill in a tray and then slide the
tray in!!!
2) After finding the right machine, get a $1 or $5 bill. Start crumpling
up into a ball. Then smooth out the bill, now it should have a very wrinkly
surface.
3) Now the hard part. You must tear a notch in the bill on the
left side about 1/2 inch below the little 1 dollar symbol (See Figure).
4) If you have done all of this right then take the bill and go out the
machine. Put the bill in the machine and wait. What should happen is:
when you put your bill in the machine it thinks everything is fine.
When it gets to the part of the bill with the notch cut out, the
machine will reject the bill and (if you have done it right)
give you the change at the same time!!! So, you end up getting your bill
back, plus the change!! It might take a little practice, but once
you get the hang of it, you can get a lot of money!

```
          !--------------------------------!
          !                                !
          ! (1)        /-------\      (1)  !
          !           !       !            !
          !           !  Pic. !            !
          ! (1)  /\    \-------/      (1)  !
          !     !!                         !
          !-----/  \-----------------------!
                \-------Make notch here. About 1/2 " down from (1)
```

P.S. Sorry for the "text work" but you should be able to get the
idea. Have fun!!! -----------------------Jolly Roger

Downloaded From P-80 International Information Systems 304-744-2253

The Basics of Hacking II

Basics to know before doing anything, essential to your continuing career as one of the elite in the country... This article, "the introduction to the world of hacking" is meant to help you by telling you how not to get caught, what not to do on a computer system, what type of equipment should I know about now, and just a little on the history, past present future, of the hacker.

Welcome to the world of hacking! We, the people who live outside of the normal rules, and have been scorned and even arrested by those from the 'civilized world', are becomming scarcer every day. This is due to the greater fear of what a good hacker (skill wise, no moral judgements here)|can do nowadays, thus causing anti- hacker sentiment in the masses. Also, few hackers seem to actually know about the computer systems they hack, or what equipment they will run into on the front end, or what they could do wrong on a system to alert the 'higher' authorities who monitor the system. This article is intended to tell you about some things not to do, even before you get on the system. I will tell you about the new wave of front end security devices that are beginning to be used on computers.

I will attempt to instill in you a second identity, to be brought up at time of great need, to pull you out of trouble. And, by the way, I take no, repeat, no, responcibility for what we say in this and the forthcoming articles. Enough of the bullshit, on to the fun: after logging on your favorite bbs, you see on the high access board a phone number! It says it's a great system to "fuck around with!" This may be true, but how many other people are going to call the same number? So: try to avoid calling a number given to the public. This is because there are at least every other user calling, and how many other boards will that number spread to? If you call a number far, far away, and you plan on going thru an extender or a re-seller, don't keep calling the same access number (I.E. As you would if you had a hacker running), this looks very suspicious and can make life miserable when the phone bill comes in the mail. Most cities have a variety of access numbers and services, so use as many as you can. Never trust a change in the system... The 414's, the assholes, were caught for this reason: when one of them connected to the system, there was nothing good there. The next time, there was a trek game stuck right in their way! They proceded to play said game for two, say two and a half hours, while telenet was tracing them! Nice job, don't you think? If anything looks suspicious, drop the line immediately!! As in, yesterday!! The point we're trying to get accross is: if you use a little common sence, you won't get busted. Let the little kids who aren't smart enough to recognize a trap get busted, it will take the heat off of the real hackers. Now, let's say you get on a computer system... It looks great, checks out, everything seems fine. Ok, now is when it gets more dangerous. You have to know the computer system to know what not to do. Basically, keep away from any command something, copy a new file into the account, or whatever! Always leave the account in the same status you logged in with. Change *nothing*... If it isn't an account with priv's, then don't try any commands that require them! All, yes all, systems are going to be keeping log files of what users are doing, and that will show up. It is just like dropping a trouble-card in an ESS system, after sending that nice operator a pretty tone. Spend no excessive amounts of time on the account in one stretch. Keep your calling to the very late night ifpossible, or during business hours (believe it or not!). It so happens that there are more users on during business hours, and it is very difficult to read a log file with 60 users doing many commnds every minute. Try to avoid systems where everyone knows each other, don't try to bluff. And above all: never act like you own the system, or are the best there is. They always grab the people who's heads swell... There is some very interesting front end equipment around nowadays, but first let's define terms... By front end, we mean any device that you must pass thru to get at the real computer. There are devices that are made to defeat hacker programs, and just plain old multiplexers. To defeat hacker programs, there are now devices that pick up the phone and just sit there... This means that your device gets no carrier, thus you think there isn't a computer on the other end. The only way around it is to detect when it was picked up. If it pickes up after the same number ring, then you know it is a hacker-defeater. These devices take a multi-digit code to let you into the system. Some are, in fact, quite sophisticated to the point where it will also limit the user name's down, so only one name or set of names can be valid logins after they input the code... Other devices input a

number code, and then they dial back a pre-programmed number for that code.
These systems are best to leave alone,
because they know someone is playing with their phone. You may think "but
i'll just reprogram the dial-back." Think again, how stupid that is...
Then they have your number, or a test loop if you were just a little
smarter. If it's your number, they have your balls (if male...),
If its a loop, then you are screwed again, since those loops
are *monitored*. As for multiplexers... What a plexer is supposed
to do is this:
The system can accept multiple users. We have to time share, so we'll let
the front-end processor do it... Well, this is what a multiplexer does.
Usually they will ask for something like "enter class" or "line:". Usually
it is programmed for a double digit number, or a four to five letter word.
There are usually a few sets of numbers it accepts, but those numbers also
set your 300/1200/2400 baud data type.
These multiplexers are inconvenient at best, so not to worry. A little
about the history of hacking: hacking, by my definition, means a great
knowledge of some special area. Doctors and lawyers
are hackers of a sort, by this definition. But most often, it is
being used in the computer context, and thus we have a definition of
"anyone who has a great amount of computer or telecommunications
knowledge." You are not a hacker because you have a list of codes...
Hacking, by my definition, has then been around only about 15 years.
It started, where else but, mit and colleges where they had computer
science or electrical engineering departments.
Hackers have created some of the best computer languages, the
most awesome operating systems, and even gone on to make millions.
Hacking used to have a good name, when we could honestly say
"we know what we are doing". Now it means (in the public eye):
the 414's, ron austin, the nasa hackers, the arpanet hackers...
All the people who have been caught,
have done damage, and are now going to have to face fines and sentences.
Thus we come past the moralistic crap, and to our purpose: educate the
hacker community, return to the days when people actually knew something...

Hacking DEC's

In this article you will learn how to log in to dec's, logging out, and all
the fun stuff to do in-between. All of this information is based on a
standard dec system.
Since there are dec systems 10 and 20, and I favor, the dec 20,
there will be more info on them in this article. It just so happens
that the dec 20 is also the more common of the two, and is used by much
more interesting people (if you know what I mean...) Ok, the first thing
you want to do when you are receiving carrier from a dec system is to find
out the format of login names. You can do this by looking at who is on the
system.
Dec=> ` (the 'exec' level prompt)
you=> sy
sy is short for sy(stat) and shows you the system status.
You should see the format of login names...
A systat usually comes up in this form:

job line program user
job: the job number (not important unless you want to log them off later)
line: what line they are on (used to talk to them...)
These are both two or three digit numbers.
Program: what program are they running under? If it says 'exec'
they aren't doing anything at all...
User: ahhhahhhh! This is the user name they are logged in under...
Copy the format, and hack yourself outa working code... Login format is as
such:

```
dec=> `
you=> login username password
```

username is the username in the format you saw above in the systat.
After you hit the space after your username, it will stop echoing
characters back to your screen. This is the password you are typing in...
Remember, people usually use their name, their dog's name, the name of a
favorite character in a book, or something like this. A few clever
people have it set to a key cluster (qwerty or asdfg). Pw's can be from 1
to 8 characters long, anything after that is ignored. You are finally in...
It would be nice to have a little help, wouldn't it? Just type a ? Or the
word help, and it will give you a whole list of topics...
Some handy characters for you to know would be the control keys,
wouldn't it? Backspace on a dec 20 is rub which is 255 on your ascii chart.
On the dec 10 it is cntrl-h. To abort a long listing or a program,
cntrl-c works fine. Use cntrl-o to stop long output to the terminal.
This is handy when playing a game, but you don't want to cntrl-c out.
Cntrl-t for the time. Cntrl-u will kill the whole line you are typing at
the moment. You may accidently run a program where the only way out is
a cntrl-x, so keep that in reserve. Cntrl-s to stop listing, cntrl-q to
continue on both systems. Is your terminal having trouble??
Like, it pauses for no reason, or it doesn't backspace right? This is
because both systems support many terminals, and you haven't told it what
yours is yet... You are using a vt05
so you need to tell it you are one.

```
Dec=> `
you=> information terminal
or...
You=> info
this shows you what your terminal is set up as...
Dec=>all sorts of shit, then the `
you=> set ter vt05 this sets your terminal
type to vt05.
```

Now let's see what is in the account (here after abbreviated acct.)
that you have hacked onto... Say

```
=> dir
```

short for directory, it shows
you what the user of the code has save to the disk. There should be a format
like this: xxxxx.Oooxxxxxx is the file name, from 1 to 20 characters
long. Ooo is the file type, one of: exe, txt, dat, bas, cmd   and a few
others that are system dependant.
Exe is a compiled program that can be run (just by typing its name at the `).
Txt is a text file, which you can see by

```
typing=>
type xxxxx.Txt
Do not try to=>
type xxxxx.Exe this is very bad for your terminal and will tell you
```

absolutly nothing.
Dat is data they have saved.
Bas is a basic program, you can have it typed out for you.
Cmd is a command type file, a little too
complicated to go into here.
Try =>
take xxxxx.Cmd
By the way, there are other users out there who may have files you can use
(gee, why else am I here?).
Type => dir <*.*> (Dec 20)
     => dir [*,*]   (dec 10)
* is a wildcard, and will allow you to access the files on other accounts
if the user has it set for public access. If it isn't set for public access,
then you won't see it. To run that program:
dec=> `
you=> username program-name
username is the directory you saw the
file listed under, and file name was
what else but the file name?
** You are not alone **
remember, you said (at the very start) sy short for systat,
and how we said this showed the other users on the system? Well, you
can talk to them, or at least send a message to anyone you see listed in a
systat. You can do this by:
dec=> the user list (from your systat)
you=> talkusername (dec 20)
      send username (dec 10)
talk allows you and them immediate transmission of whatever you/they type
to be sent to the other. Send only allow you one message to be sent, and
send, they will send back to you, with talk you can just keep going. By the
way, you may be noticing with the talk command that what you type is still
acted upon by the parser (control program). To avoid the constant error
messages type either:
you=> ;your message
you=> rem your message
the semi-colon tells the parser that what follows is just a comment. Rem
is short for 'remark' and ignores you from then on until you type a cntrl-z
or cntrl-c, at which point it puts you back in the exec mode. To break the
connection from a talk command type:
you=> break priv's:
if you happen to have privs, you can do all sorts of things.
First of all, you have to activate those privs.
You=> enable
this gives you a $ prompt, and allows you to do this:
whatever you can do to your own directory you can now do to any
other directory. To create a new acct. Using your privs, just type
=>build username
if username is old, you can edit it, if it is new, you can
define it to be whatever you wish. Privacy means nothing to a user with
privs. By the way, there are various levels of privs: operator, wheel,
cia.
wheel is the most powerful, being that he can log in from anywhere and
have his powers.
Operators have their power because they are at a special terminal
allowing them the privs. Cia is short for 'confidential information

access', which allows you a low level amount of privs.
Not to worry though, since you can read the system log file, which also
has the passwords to all the other accounts.
To de-activate your privs, type
you=> disable
when you have played your greedy heart out, you can finally leave the
system with the command=>
logout
this logs the job you are using off the system (there may be varients
of this such as kjob, or killjob).

Jackpotting ATM Machines

JACKPO
TTING was done rather successfully a while back in (you guessed it)
New York. What the culprits did was:
Sever (actually cross over) the line between the ATM and the
host. insert a microcomputer between the ATM and the host. insert
a fradulent card into the ATM. (card=cash card, not hardware)
What the ATM did was: send a signal to the host, saying "Hey! Can I
give this guy money, or is he broke, or is his card invalid?"
What the microcomputer did was: intercept the signal from the host,
discard it, send "there's no one using the ATM" signal.
What the host did was: get the "no one using" signal, send back "okay,
then for God's sake don't spit out any money!" signal to ATM.
What the microcomputer did was:
intercept signal (again), throw it away (again), send "Wow! That
guy is like TOO rich! Give him as much money as he wants. In
fact, he's so loaded, give him ALL the cash we have! He is
really a valued customer." signal.
What the ATM did:
what else? Obediently dispense cash till the cows came home (or
very nearly so).
What the crooks got:
well in excess of $120,000 (for one weekend's work), and several
years when they were caught.
This story was used at a CRYPTOGRAPHY conference I attended a while
ago to demonstrate the need for better information security. The
lines between ATM's & their hosts are usually 'weak' in the sense that
the information transmitted on them is generally not encrypted in any
way. One of the ways that JACKPOTTING can be defeated is to encrypt
the information passing between the ATM and the host. As long as the
key cannot be determined from the ciphertext, the transmission (and
hence the transaction) is secure.
A more believable, technically accurate story might concern a person
who uses a computer between the ATM and the host to determine the key
before actually fooling the host. As everyone knows, people find
cryptanalysis a very exciting and engrossing subject...don't they?
(Hee-Hee)

```
_____        ______
|   |-<<-|   |-<<-|    |
|ATM|    micro    |Host|
|___|->>-|   |->>-|____|
```

The B of A ATM's are connected through dedicated lines to a host computer as the Bishop said. However, for maintenance purposes, there is at least one separate dial-up line also going to that same host computer. This guy basically bs'ed his way over the phone till he found someone stupid enough to give him th number. After finding that, he had has Apple hack at the code. Simple.

Step 2: He had a friend go to an ATM with any B of A ATM card. He stayed at home with the Apple connected to the host. When his friend inserted the card, the host displayed it. The guy with the Apple modified the status & number of the card directly in the host's memory. He turned the card into a security card, used for testing purposes. At that point, the ATM did whatever it's operator told it to do.

The next day, he went into the bank with the $2000 he received, talked to the manager and told him every detail of what he'd done. The manager gave him his business card and told him that he had a job waiting for him when he got out of school.

Now, B of A has been warned, they might have changed the system. On the other hand, it'd be awful expensive to do that over the whole country when only a handful of people have the resources and even less have the intelligence to duplicate the feat. Who knows?

How to grow Marijuana

MARIJUANA

Marijuana is a deciduous plant which grows from seeds. The fibrous section of the plant was (has been replaced by synthetics) used to make rope. The flowering tops, leaves, seeds, and resin of the plant is used by just about everyone to get HIGH.

Normally, the vegetable parts of the plant are smoked to produce this "high," but thay can also be eaten. The axtive ingredient in marijuana resin is THC (tetahydrocannabinol). Marijuana contains from 1 - 4 per cent THC (4 per cent must be considered GOOD dope).

Marijuana grows wild in many parts of the world, and is cultivated in Mexice, Vietnam, Africa, Nepal, India, South America, etc.,etc. The marijuana sold in the United States comes primarily from, yes, the Uniited States.

It is estimated that at least 50 per cent of the grass on the streets in America is homegrown. The next largest bunch comes actoss the borders from Mexico, with smaller amounts filtering in from Panama, occasionally South America, and occasinally, Africa.

Hashish is the pure resin of the marijuana plant, which is scraped from the flowering tops of the plant and lumped together. Ganja is the ground-up tops of the finest plants. (It is also the name given to any sort of marijuana in Jamaica.)

Marijuana will deteriorate in about two years if exposed to light, air or heat. It should always be stored in cool places.

Grass prices in the United States are a direct reflection of the laws of supply and demand (and you thought that high school economics would never be useful). A series of large border busts, a short growing season, a bad crop, any number of things can drive the price of marijuana up. Demand still seems to be on the increase in the U.S., so prices seldom fall below last year's level.

Each year a small seasonal drought occurs, as last year's supply runs low, and next year's crop is not up yet. Prices usually rase about 20 - 75 per cent during this time and then fall back to "normal."

Unquestionably, a large shortage of grass causes a percentage of smokers to turn to harder drugs instead. For this reason, no grass control program can ever be beneficial or "successful."

GROW IT!

There is one surefire way of avoiding high prices and the grass DT's: Grow your own. This is not as difficult as some "authorities" on the subject would make you believe. Marijuana is a weed, and a fairly vivacious one at that, and it will grow almost in spite of you.

OUTDOORS

Contrary to propular belief, grass grows well in many place on the North American continent. It will flourish even if the temperature does not raise above 75 degrees.

The plants do need a minimum of eight hours of sunlight per day and should be planted in late April/early May, BUT DEFINITELY, after the last frost of the year.

Growing an outdoor, or "au naturel", crop has been the favored method over the years, because grass seems to grow better without as much attention when in its natural habitat.

Of course, an outdoors setting requires special precautions not encountered with an indoors crop; you must be able to avoid detection, both from law enforcement freaks and common freaks, both of whom will take your weed and probably use it. Of course, one will also arrest you. You must also have access to the area to prepare the soil and harvest the crop.

There are two schools of thought about starting the seeds. One says you should start the seedlings for about ten days in an indoor starter box (see the indoor section) and then transplant. The other theory is that you should just start them in the correct location. Fewer plants will come up with this method, but there is no shock of transplant to kill some of the seedlings halfway through.

The soil should be preprepared for the little devils by turning it over a couple of times and adding about one cup of hydrated lime per square yard of soil and a little bit (not too much, now) of good water soluble nitrogen fertilizer. The soil should now be watered several times and left to sit about one week.

The plants should be planted at least three feet apart, getting too greedy and stacking them too close will result in stunted plants.

The plants like some water during their growing season, BUT not too much. This is especially true around the roots, as too much water will rot the root system.

Grass grows well in corn or hops, and these plants will help provide some camouflage. It does not grow well with rye, spinach, or pepperweed.

It is probally a good idea to plant in many small, broken patches, as people tend to notice patterns.

GENERAL GROWING INFO

Both the male and he female plant produce THC resin, although the male is not as strong as the female. In a good crop, the male will still be plenty smokable and should not be thrown away under any circumstances.

Marijuana can reach a hight of twenty feet (or would you rather wish on a star) and obtain a diameter of 4 1/2 inches. If normal, it has a sex ratio of about 1:1, but this can be altered in several ways.

The male plant dies in the 12th week of growing, the female will live another 3 - 5 weeks to produce her younguns. Females can weigh twice as much as males when they are mature.

Marijuana soil should compact when you squeeze it, but should also break apart with a small pressure and absorb water well. A nice test for either indoor or outdoor growing is to add a bunch of worms to the soil, if they live and hang aroung, it is good soil, but if they don't, well, change it. Worms also help keep the soil loose enough for the plants to grow well.

SEEDS

To get good grass, you should start with the right seeds. A nice starting point is to save the seeds form the best batch you have consumed. The seeds should be virile, that is, they should not be grey and shiriveled up, but green, meaty, and healthy appearing. A nice test is to drop the seeds on a hot frying pan. If they "CRACK," they are probably good for planting purposes.

The seeds should be soaked in distilled water overnight before planting. BE SURE to plant in the ground with the pointy end UP. Plant about 1/2" deep. Healthy seeds will sprout in about five days.

SPROUTING

The best all around sprouting method is probably to make a sprouting box (as sold in nurseries) with a slated bottom or use paper cups with holes punched in the bottoms. The sprouting soil should be a mixture of humus, soil, and five sand with a bit of organic fertilizer and water mixed in about one week before planting.

When ready to transplant, you must be sure and leave a ball of soil around the roots of each plant. This whole ball is dropped into a baseball-sized hold in the permanent soil.

If you are growing/transplanting indoors, you should use a green safe light (purchased at nurseries) during the transplanting operation.

If you are transplanting outdoors, you should time it about two hours befor sunset to avoid damage to the plant. Always wear cotton gloves when handling the young plants.

After the plants are set in the hole, you should water them. It is also a good idea to use a commercial transplant chemical (also purchased at nurseries) to help then overcome the shock.

INDOOR GROWING

Indoor growing has many advantages, besides the apparent fact that it is much harder to have your crop "found," you can control the ambient conditions just exactly as you want them and get a guaranteed "good" plant.

Plants grown indoors will not appear the same as their outdoor cousins. They will be scrawnier appearing with a weak stems and may even require you to tie them to a growing post to remain upright, BUT THEY WILL HAVE AS MUCH OR MORE RESIN!

If growing in a room, you should put tar paper on the floors and then buy sterilized bags of soil form a nursery. You will need about one cubic foot of soil for eavh plant.

The plants will need about 150 ml. of water per plant/per week. They will also need fresh air, so the room must be ventilated. (however, the fresh air should contain NO TOBACCO smoke.)

At least eight hours of light a day must be provided. As you increase the light, the plants grow faster and show more females/less males. Sixteen hours of light per day seems to be the best combination, beyond this makes little or no appreciable difference in the plant quality.

Another idea is to interrupt the night cycle with about one hour of light. This gives you more females.

The walls of your growing room should be painted white or covered with aluminum foil to reflect the light.

The lights themselves can be either bulbs of fluorescent. Figure about 75 watts per plant or one plant per two feet of flouresent tube.

The fluorescents are the best, but do not use "cool white" types. The light sources should be an average of twenty inches from the plant and NEVER closer than 14 inches. They may be mounted on a rack and moved every few days as the plants grow.

The very best light sources are those made by Sylvania and others especially for growing plants (such as the "gro lux" types).

HARVESTING AND DRYING

The male plants will be taller and have about five green or yellow sepals, which will split open to fertilize the female plant with pollen.

The female plant is shorter and has a small pistillate flower, which really doesn't look like a flower at all but rather a small bunch of leaves in a cluster.

If you don't want any seeds, just good dope, you should pick the males before they shed their pollen as the female will use some of her resin to make the seeds.

After another three to five weeks, after the males are gone, the females will begin to wither and die (from loneliness?), this is the time to pick.

In some nefarious Middle Eastren countries, farmers reportedly put their beehives next to fiels of marijuana. The little devils collect the grass pollen for their honey, which is supposed to contain a fair dosage of THC.

The honey is then enjoyed by conventional methods or made into ambrosia.

If you want seeds - let the males shed his pollen then pick him. Let the female go another month and pick her.

To cure the plants, they must be dried. On large crops, this is accomplished by constructing a drying box or drying room.

You must have a heat source (such as an electric heater) which will make the box/room each 130 degrees. The box/room must be ventilated to carry off the water-vapor-laden air and replace it with fresh.

A good box can be constructed from an orange crate with fiberglass insulated walls, vents in the tops, and screen shelves to hold the leaves.

There must be a baffle between the leaves and the heat source.
A quick cure for smaller amounts is to: cut the plant at the soil level and wrap it in a cloth so as not to loose any leavs. Take out any seeds by hand and store. Place all the leaves on a cookie sheet or aluminum foil and put them in the middle sheld of the oven, which is set on "broil." In a few seconds, the leaves will smoke and curl up, stir them around and give another ten seconds before you take them out.

TO INCREASE THE GOOD STUFF

There are several tricks to increase the number of females, or the THC content of plants:
You can make the plants mature in 36 days if you are in a hurry, by cutting back on the light to about 14 hours, but the plants will not be as big.
You should gradually shorten the light cycle until you reach fourteen hours.
You can stop any watering as the plants begin to bake the resin rise to the flowers. This will increse the resin a bit.
You can use a sunlamp on the plants as they begin to develop flower stalks.
You can snip off the flower, right at the spot where it joins the plant, and a new flower will form in a couple of weeks.
This can be repeated two or three times to get several times more flowers than usual.
If the plants are sprayed with Ethrel early in their growing stage, they will produce almost all female plants. This usually speeds up the flowering also, it may happen in as little as two weeks.
You can employ a growth changer called colchicine. This is a bit hard to get and expensive. (Should be ordered through a lab of some sort and costs about $35 a gram.)
To use the colchicine, you should prepare your presoaking solution of distilled water with about 0.10 per cent colchicine. This will cause many of the seeds to die and not germinate, but the ones that do come up will be polyploid plants. This is the accepted difference between such strains as "gold" and normal grass, and yours will DEFINITELY be superweed.
The problem here is that colchicine is a posion in larger quanities and may be poisonous in the first generation of plants. Bill Frake, author of CONNOISSEUR'S HANDBOOK OF MARIJUANA runs a very complete colchicine treatment down and warns against smoking the first generation plants (all succeeding generations will also be polyploid) bacause of this poisonous quality.
However, the Medical Index shows colchicine being given in very small quantities to people for treatment if various ailments. Although these quantities are small, they would appear to be larger than any you could recive form smoaking a seed-treated plant.
It would be a good idea to buy a copy of CONNOISSEUR'S, if you are planning to attempt this, and read Mr. Drake's complete instructions.
Another still-experimental process to increase the resin it to pinch off the leaf tips as soon as they appear from the time the plant is in the seedling stage on through its entire life-span. This produces a distorted, wrecked-looking plant which would be very difficuly to recognize as marijuana. Of course, there is less substance to this plant, but such

wrecked creatures have been known to produve so much resin that it crystallizes a strong hash all over the surface of the plant - might be wise to try it on a plant or two and see what happens.

PLANT PROBLEM CHART

Always check the overall enviromental conditions prior to passing judgment - soil aroung 7 pH or slightly less - plenty of water, light, fresh air, loose soil, no water standing in pools.

SYMPTOM	PROBABLY PROBLEM/CURE
Larger leaves turning yellow - smaller leaves still green.	Nitrogen dificiency - add nitrate of soda or organic fertilizer.
Older leaves will curl at edges, turn dark, possibaly with a purple cast.	Phosphorsus dificiency - add commercial phosphate.
Mature leaves develop a yellowish cast to least veinal areas.	Magnesium dificiency - add commercial fertilizer with a magnesium content.
Mature leaves turn yellow and then become spotted with edge areas turning dark grey.	Potassium dificiency - add muriate of potash.
Cracked stems, no healthy support tissue.	Boron dificiency - add any plant food containing boron.
Small wrinkled leaves with yelloish vein systems.	Zinc dificiency - add commercial plant food containing zinc.
Young leaves become deformed, possibaly yellowing.	Molybedum dificiency - use any plant food with a bit of molydbenum in it.

EXTRA SECTION:
BAD WEED/GOOD WEED

Can you turn bad weed into good weed? Surprisingly enough, the answer to this oft-asked inquiry is, yes!

Like most other things in life, the amount of good you are going to do relates directly to how much effort you are going to put into it. There are no instant, supermarket products which you can spray on Kansas catnip and have wonderweed, but there are a number of simplified, inexpensive processes (Gee, Mr. Wizard!) thich will enhance mediocre grass somewhat, ant there are a couple of fairly involved processes which will do up even almost-parsley weed into something worth writing home about.

EASES

1. Place the dope in a container which allows air to enter in a restricted fashion (such as a can with nail holes punched in its lid) and add a bunch of dry ice, and the place the whold shebang in the freezer for a few days. This process will add a certain amount of potency to the product, however, this only works with dry ice, if you use normal, everyday

freezer ice, you will end up with a soggy mess...
2. Take a quantity of grass and dampen it, place in a baggie or another socially acceptable container, and store it in a dark, dampish place for a couple of weeks (burying it also seems to work). The grass will develop a mold which tastes a bit harsh, a and burns a tiny bit funny, but does increase the potency.
3. Expose the grass to the high intensity light of a sunlamp for a full day or so. Personally, I don't feel that this is worth the effort, but if you just spent $400 of your friend's money for this brick of super-Colombian, right-from-the-President's-personal-stash, and it turns out to be Missouri weed, and you're packing your bags to leave town before the people arrive for their shares, well, you might at least try it. Can't hurt.
4. Take the undisirable portions of our stash (stems, seeds, weak weed, worms, etc.) and place them in a covered pot, with enough rubbing alchol to cover everything.
Now CAREFULLY boil the mixture on an ELECTRIC stove or lab burner. DO NOT USE GAS - the alchol is too flammable. After 45 minutes of heat, remove the pot and strain the solids out, SAVING THE ALCOHOL.
Now, repeat the process with the same residuals, but fresh alchol.
When the second boil is over, remove the solids again, combine the two quantities of alcohol and reboil until you have a syrupy mixture.
Now, this syrupy mixture will contain much of the THC formerly hidden in the stems and such. One simply takes this syrup the throughly combines it with the grass that one wishes to improve upon.

SPECIAL SECTION ON RELATED SUBJECT MARYGIN:

Marygin is an anagram of the words marijuana and gin, as in Eli Whitney.
It is a plastic tumbler which acts much like a commercial cottin gin.
One takes about one ounce of an harb and breaks it up. This is then placed in the Marygin and the protuding knod is roatated. This action turns the internal wheel, which separates the grass from the debris (seeds, stems).
It does not pulberize the grass as screens have a habit of doing and is easily washable.
Marygin is available from:

P.O. Box 5827
Tuscon, Arizona 85703
$5.00

GRASS
Edmund Scientific Company
555 Edscorp Building
Barrington, New Jersy 08007

Free Catalog is a wonder of good things for the potential grass grower. They have an electric thermostat greenhouse for starting plants for a mere $14.95.
Soil test kits for PH - $2.40
Al test - $9.95
Soil thermometer - $2.75
Lights which approzimate the true color balance of the sun and are probably the most beneficial types available: 40 watt, 48 inch - 4 for $15.75.
Indoor sun bulb, 75 or 150 watt - $5.75.
And, they have a natural growth regualtor for plants (Gibberellin) which can change height, speed growth, and maturity, promote blossoming,

etc. Each plant reacts differently to treatment with Gibberellin...there's no fun like experimenting - $2.00

SUGGESTED READING

THE CONNOISSEUR'S HANDBOOK OF MARIJUANA, Bill Drake
Straight Arrow Publishing - $3.50
625 Third Street
San Francisco, California

FLASH
P.O.Box 16098
San Fransicso, California 94116
Stocks a series of pamphlets on grass, dope manufacture, cooking.
Includes the Mary Jane Superweed series.

Downloaded From P-80 International Information Systems 304-744-2253

How To Create A New Indentity

You might be saying, "Hey Glitch, what do I need a new identity for?" The answer is simple. You might want to go buy liquor somewhere, right? You might want to go give the cops the false name when you get busted so you keep your good name, eh? You might even want to use the new identity for getting a P.O. Box for carding. Sure! You might even want the stuff for renting yourself a VCR at some dickless loser of a convenience store. Here we go:
Getting a new ID isn't always easy, no one said it would be. By following these steps, any bozo can become a new bozo in a coupla weeks.

STEP 1

The first step is to find out who exactly you'll become. The most secure way is to use someone's ID who doesn't use it themselves. The people who fit that bill the best are dead. As an added bonus they don't go complaining one bit. Go to the library and look through old death notices. You have to find someone who was born about the same time as you were, or better yet, a year or two older so you can buy booze, etc. You should go back as far as you can for the death because most states now cross index deaths to births so people can't do this in the future. The cutoff date in Wisconsin is 1979, folks in this grand state gotta look in 1978 or earlier. Anything earier there is cool. Now, this is the hardest part if you're younger. Brats that young happen to be quite resilient, takin' falls out of three story windows and eating rat poison like its Easter candy, and not a scratch or dent. There ain't many that die, so ya gotta look your ass off. Go down to the library and look up all the death notices you can, if it's on microfilm so much the better. You might have to go through months of death notices though, but the results are well worth it. You gotta get someone who died locally in most instances: the death certificate is filed only in the county of death. Now you go down to the county courthouse in the county where he died and get the death certificate, this will cost you around $3-$5 depending on the state you're in. Look at this hunk of paper, it could be your way to vanish in a clould of smoke when the right time comes, like right after that big scam. If You're lucky, the slobs parents signed him up with social security when he was a snot nosed brat. That'll be another piece of ID you can get. If not, thats ok too. It'll be listed on the death certificate if he has one. If you're lucky, the stiff was born locally and you can get his birth certificate right away.

STEP 2

Now check the place of birth on the death certificate, if it's in the same place you standing now you're all set. If not, you can mail away for one from that county but its a minor pain and it might take a while to get, the librarian at the desk has listings of where to write for this stuff and exactly how much it costs. Get the Birth cirtificate, its worth the extra money to get it certified because thats the only way some people will accept it for ID. When yur gettin this stuff the little forms ask for the reason you want it, instead of writing in "Fuck you", try putting in the word "Geneology". They get this all the time. If the Death certificate looks good for you, wait a day or so before getting the certified birth certificate in case they recognize someone wanting it for a dead guy.

STEP 3

Now your cookin! You got your start and the next part's easy. Crank out your old Dot matrix printer and run off some mailing labels addressed to you at some phony address. Take the time to check your phony address that there is such a place. Hotels that rent by the month or large apartment buildings are good, be sure to get the right zip code for the area. These are things that the cops might notice that will trip you up. Grab some old junk mail and paste your new lables on them. Now take them along with the birth certificate down to the library. Get a new library card. If they ask you if you had one before say that you really aren't sure because your family moved around alot when you were a kid. Most libraries will allow you to use letters as a form of ID when you get your card. If they want more give them a sob story about how you were mugged and got your wallet stolen with all your identification. Your card should be waiting for you in about two weeks. Most libraries ask for two forms of ID, one can be your trusty Birth Certificate, and they do allow letters addressed to you as a second form.

STEP 4

Now you got a start, it isn't perfect yet, so let's continue. You should have two forms of ID now. Throw away the old letters, or better yet stuff them inside the wallet you intend to use with this stuff. Go to the county courthouse and show them what nice ID you got and get a state ID card. Now you got a picture ID. This will take about two weeks and cost about $5, its well worth it.

STEP 5

If the death certificate had a social security number on it you can go out and buy one of those metal SS# cards that they sell.
If it didn't, then you got all kinds of pretty ID that shows exactly who you are. If you don't yet have an SS#, Go down and apply for one, these are free but they could take five or six weeks to get, Bureaucrats you know... You can invent a SS# too if ya like, but the motto of 'THE WALKING GLITCH' has always been "Why not excellence?".

STEP 6

If you want to go whole hog you can now get a bank account in your new name. If you plan to do alot of traveling then you can put alot of money in the account and then say you lost the account book. After you get the new book you take out all the cash. They'll hit you with a slight charge and maybe tie-up your money some, but if you're ever broke in some small town that bank book will keep you from being thrown in jail as a vagrant.

ALL DONE?

So kiddies, you got ID for buying booze, but what else? In some towns (the larger the more likely) the cops if they catch you for something petty like shoplifting stuff under a certain dollar amount, will just give you a ticket, same thing for pissing in the street. Thats it!
No fingerprints or nothing, just pay the fine (almost always over $100) or appear in court. Of course they run a radio check on your ID, you'll be clean and your alter-ego gets a blot on his record.
Your free and clear. Thats worth the price of the trouble you've gone through right there. If your smart, you'll toss that ID away if this happens, or better yet, tear off your picture and give the ID to someone you don't like, maybe they'll get busted with it.
If you're a working stiff, here's a way to stretch your dollar. Go to work for as long as it takes to get unemployment and then get yourself fired.
Go to work under the other name while your getting the unemployment.
With a couple of sets of ID, you can live like a king.

The Infinity Transmitter

FROM THE BOOK BUILD YOUR OWN
LASER, PHASER, ION RAY GUN & OTHER WORKING SPACE-AGE PROJECTS

Description: Briefly, the Infinity Transmitter is a device which activates a microphone via a phone call. It is plugged into the phone line, and when the phone rings, it will immediately intercept the ring and broadcast into the phone any sound that is in the room. This device was originally made by Information Unlimited, and had a touch tone decoder to prevent all who did not know the code from being able to use the phone in its normal way. This version, however, will activate the microphone for anyone who calls while it is in operation.
NOTE: It is illegal to use this device to try to bug someone. It is also pretty stupid because they are fairly noticeable.

Parts List:
Pretend that uF means micro Farad, cap= capacitor

Part	#	Description
----	-	-----------
R1,4,8	3	390 k 1/4 watt resistor
R2	1	5.6 M 1/4 watt resistor
R3,5,6	3	6.8 k 1/4 watt resistor
R7/S1	1	5 k pot/switch
R9,16	2	100 k 1/4 watt resistor
R10	1	2.2 k 1/4 watt resistor
R13,18	2	1 k 1/4 watt resistor
R14	1	470 ohm 1/4 watt resistor
R15	1	10 k 1/4 watt resistor
R17	1	1 M 1/4 watt resistor
C1	1	.05 uF/25 V disc cap
C2,3,5,6,7	5	1 uF 50 V electrolytic cap or tant (preferably non-polarized)
C4,11,12	3	.01 uF/50 V disc cap
C8,10	2	100 uF @ 25 V electrolytic cap
C9	1	5 uF @ 150 V electrolytic cap
C13	1	10 uF @ 25 V electrolytic cap
TM1	1	555 timer dip
A1	1	CA3018 amp array in can
Q1,2	2	PN2222 npn sil transistor
Q3	1	D4OD5 npn pwr tab transistor
D1,2	2	50 V 1 amp react. 1N4002
T1	1	1.5 k/500 matching transformer
M1	1	large crystal microphone
J1	1	Phono jack optional for sense output
WR3	(24")	#24 red and black hook up wire
WR4	(24")	#24 black hook up wire
CL3,4	2	Alligator clips
CL1,2	2	6" battery snap clips
PB1	1	1 3/4x4 1/2x.1 perfboard
CA1	1	5 1/4x3x2 1/8 grey enclosure fab
WR15	(12")	#24 buss wire
KN1	1	small plastic knob
BU1	1	small clamp bushing
B1,2	2	9 volt transistor battery or 9V ni-cad

Circuit Operation: Not being the most technical guy in the world, and not being very good at electronics (yet), I'm just repeating what Mr. Iannini's said about the circuit operation. The Transmitter consists of a high grain amplifier fed into the telephone lines via transformer. The circuit is initiated by the action of a voltage transient pulse occurring across the phone line at the instant the telephone circuit is made (the ring, in other words). This transient immediately triggers a timer whose output pin 3 goes positive, turning on transistors Q2 and Q3. Timer TM1 now remains in this state for a period depending on the values of R17 and C13 (usually about 10 seconds for the values shown). When Q3 is turned on by the timer, a simulated "off hook" condition is created by the switching action of Q3 connecting the 500 ohm winding of the transformer directly across the phone lines. Simultaneously, Q2 clamps the ground of A1, amplifier, and Q1, output transistor, to the negative return of B1,B2, therefore enabling this amplifier section. Note that B2 is always required by supplying quiescent power to TM1 during normal conditions. System is off/on controlled by S1 (switch).

A crystal mike picks up the sounds that are fed to the first two transistors of the A1 array connected as an emitter follower driving the remaining two transistors as cascaded common emitters. Output of the array now drives Q1 capacitively coupled to the 1500 ohm winding of T1. R7 controls the pick up sensitivity of the system.

Diode D1 is forward biased at the instant of connection and essentially applies a negative pulse at pin 2 of TM1, initiating the cycle. D2 clamps any high positive pulses. C9 dc-isolates and desensitizes the circuit. The system described should operate when any incoming call is made without ringing the phone.

Schematic Diagram: Because this is text, this doesn't look too hot. Please use a little imagination! I will hopefully get a graphics drawing of this out as soon as I can on a Fontrix graffile.

To be able to see what everything is, this character: | should appear as a horizontal bar. I did this on a][e using a][e 80 column card, so I'm sorry if it looks kinda weird to you.

```
Symbols:
 resistor: -/\/\/-           switch: _/ _
 battery:  -|!|!-            capacitor (electrolytic): -|(-
 capacitor (disc): -||-                    _   _
 transistor:(c)  > (e)       Transformer: )||(
              \_/                          )||(
               |(b)                       _)||(_
 diode: |<
 chip: ._____.
       !_____! (chips are easy to recognize!)
```

Dots imply a connection between wires. NO DOT, NO CONNECTION.
ie.: _!_ means a connection while _|_ means no connection.

```
--------------------------------------------------------------------------

.____________________to GREEN wire phone line
|
| .___________________to RED wire phone line
| |
| |    ._______(M1)____________.
| |    |                       |
| |    |         R1            |
| |    !________/\/\/__________!
| |    |                     _!_ C1
| |    |this wire is the amp     ___
| |    |<=ground                |                 R2
| |    |                       !________________/\/\/___________.
| |    |                ._____!______.                         |
| |    !________________!4      9     11!_________________________!
| |    |                |           |                          |
| |    !________________!7          12.________________________!
| |    |                |    A1     |           R3             |
| |    !________________!10      ___*8!______.___/\/\/__________! ^
| |    |                |      /    |      |                   | |
||    |  C4          |     /     |     \               |2ma
||    !____||_______.    |    /      |     /R4              B1 +
||    |   ||    |    |    /       |    \                |!|!
||    |   R7     | C2  |  /         |     /                 |
||    !____/\/\/___!__)|__!8*_/        |     |             S1  |
||    |    ^          |          6!________!        neg<__/.__!
||    |   |   C3      |           |     | C5      return     |
||    |   !_____|(___.__!3           |     '-|(-|              |
||    |            | |     5    1!____________!               |
||    |            \  !________.________!         |           B2|!|!
||    !________.    R8 /        |              |            +
||          |     \       |               |    R6       |3ma
||          |     !__________!_____________________|_____/\/\/______! |
||          |  R5          |               |            | v
||          !__/\/\/___________|_____________________!             |
||          |             |                            |
||          |             |                            |
||          |           C6 |                             |
||          |          |-)|-'          R9                |
||          |          !__________________/\/\/________.          |
||          |          |                      |         |
||          |      Q1 _!_                     |  R10      |
||          !_____________/ \_______________________________!__/\/\/_____!
||          |                                  |         |
||          |                                  |         |
||          |       C8                           |         |
||          !__________)|_________________________________|____________!
||          !                                   |         |
||         /                                    |         |
||     -----|                                    |         |
||     |    \                                   |         |
||     |     >                                   |         |
||     |     |                                  |         |
||     |     |                                  |         |
||     |     !______________.                            |         |
||     |               |                        |         |
||     !__________.        |                     |         |
||              |      |                        |         |
| !________.       |      |                 .______!         |
|        |      |      |                 |             |
|        |      |      |                 |             |
|        |      |      |                 | C7             |
|        |      |      |                 '-|(-|           |
|        |__________|_________!________.T1._________________|          |
|               |      |  1500 )||( 500                    |
|               |      |   ohm )||( ohm                     |
|               |      !______.)||(.__.                      |
|               |      |          |                    |
|               |      |          |                    |
|               |      |           >                    |
|               |      |         |/                     |
|               |      |     +----|   Q3                  |
|               |      |     |   |\                     |
!______________________|__________|_______|______!__. D1   C9             |
                |       |     |      '-|<---|(------|       |
     ._______________!        |      |                    |        |
     |                    |      |                    |        |
     |      .__________________!      |                    |        |
     |      |                    |                    |        |
     \      |      .__________________!           C11       |        |
     /      |      |                  .___||_____________!        |
 R13 \      |      |                     |  ||           |        |
     /      |      |                  |               |        |
     \      !___.___|_________________________!              |        |
     |      |  |  |                  |    R16        |    R15  |
     |      v   |  |                  !___/\/\/\_________!___/\/\/_!
     |     neg  |  |                   |    D2          |        |
     |   return |  |                   !______|<___________!        |
     |    B1,B2 |   \                   |               |        |
     |          |  /                  |    .______________!_.       |
     |          |  \R14                 |C12 |   TM1      2 |       |
     |          |  /                  !_||_!5           4!________!
     |          |  \                  | || |            |       |
     |          |  |                  !____!1           8!________!
     |          |  |                  |    |    7 6   3  |       |
     |          |  |                  |    !______._.____._!       |
     |          |  |                  |         | |    |        |
     |          |  |                  |   C13    | |    |   R17   |
     |          |  |                  !___)|______!_!____|__/\/\/__!
     |          |  |                  |               |        |
     !_____________|___!_________________________|__________________!        |
                |  |                  |                        |
                |  \                  |         C10             |
                |  /R18                 !___________)|________________!
                |  \
                |  /
                |  |
                !___O J1
                  sense output
```

Construction notes: Because the damned book just gave a picture instead of step by step instructions, and I'll try to give you as much help as possible. Note that all the parts that you will be using are clearly labeled in the schematic. The perfboard, knobs, 'gator clips, etc are optional. I do strongly suggest that you do use the board!!! It will make wiring the components up much much easier than if you don't use it.

The knob you can use to control the pot (R7). R7 is used to tune the IT so that is sounds ok over the phone. (You get to determine what sounds good) By changing the value of C13, you can change the amount of time that the circuit will stay open (it cannot detect a hang up, so it works on a timer.) A value of 100 micro Farads will increase the time by about 10 times.

The switch (S1) determines whether or not the unit is operational. Closed is on. Open is off. The negative return is the negative terminals of the battery!! The batteries will look something like this when hooked up:

```
  <-v______.   ._______.    .______.   ._____->
        |  |      |   |     |  |
       __!___!__    |   |  __!___!__
       | +   - |    !_/ _!   | +   - |
       |       |  switch ^   |       |
| 9volts|        |   | 9volts|
!_______! neg return  !_______!
```

To hook this up to the phone line, there are three ways, depending upon what type of jack you have. If it is the old type (non modular) then you can just open up the wall plate and connect the wires from the transmitter directly to the terminals of the phone.

If you have a modular jack with four prongs, attach the red to the negative prong (don't ask me which is which! I don't have that type of jack... I've only seen them in stores), and the green to the positive prong, and plug in. Try not to shock yourself...

If you have the clip-in type jack, get double male extension cord (one with a clip on each end), and chop off one clip. Get a sharp knife and splice off the grey protective material. You should see four wires, including one green and one red. You attach the appropriate wires from the IT to these two, and plug the other end into the wall.

Getting the IT to work: If you happen to have a problem, you should attempt to do the following (these are common sense rules!!) Make sure that you have the polarity of all the capacitors right (if you used polarized capacitors, that is). Make sure that all the soldering is done well and has not short circuited something accidently (like if you have a glob touching two wires which should not be touching.) Check for other short circuits. Check to see if the battery is in right. Check to make sure the switch is closed.

If it still doesn't work, drop me a line on one of the Maryland or Virginia BBSs and I'll try to help you out.

The sense output: Somehow or other, it is possible to hook something else up to this and activate it by phone (like an alarm, flashing lights, etc.)

LSD

I think, of all the drugs on the black market today, LSD is the strangest. It is the most recent major drug to come to life in the psychedelic subculture. (Blah blah blah... let's get to the good stuff: How to make it in your kitchen!!)

1) Grind up 150 grams of Morning Glory seeds or baby Hawaiian wood rose seeds.
2) In 130 cc. of petroleum ether, soak the seeds for two days.
3) Filter the solution through a tight screen.
4) Throw away the liquid, and allow the seed mush to dry.
5) For two days allow the mush to soak in 110 cc. of wood alcohol.
6) Filter the solution again, saving the liquid and labeling it "1."
7) Resoak the mush in 110 cc. of wood alcohol for two days.
8) Filter and throw away the mush.
9) Add the liquid from the second soak to the solution labeled "1."
10) Pour the liquid into a cookie tray and allow it to

evaporate.
11) When all of the liquid has evaporated, a yellow gum remains. This should be scraped up and put into capsules.

30 grams of Morning Glory seeds = 1 trip
15 Hawaiian wood rose seeds = 1 trip

Many companies, such as Northop-King have been coating their seeds with a toxic chemical, which is poison. Order seeds from a wholesaler, as it is much safer and cheaper. Hawaiian wood rose seeds can be ordered directly from:

Chong's Nursery and Flowers
P.O. Box 2154
Honolulu, Hawaii

LSD DOSAGES

The basic dosages of acid vary according to what kind of acid is available and what medium of ingestion is used. Chemically, the potency of LSD-25 is measured in micrograms, or mics. If you're chemically minded or making your own acid, then computing the number of micrograms is very important. Usually between 500 and 800 mics is plenty for an 8 hour trip, depending on the quality of the acid, of course. I have heard of people taking as much as 1,500-2,000 mics. This is not only extremely dangerous, it is extremely wasteful.

LSD comes packaged in many different forms. The most common are listed below:

1) The brown spot, or a piece of paper with a dried drop of LSD on it, is always around. Usually one spot equals one trip.
2) Capsuled acid is very tricky, as the cap can be almost any color, size, or potency. Always ask what the acid is cut with, as a lot of acid is cut with either speed or strychnine. Also note dosage.
3) Small white or colored tablets have been known to contain acid, but, as with capsuled acid, it's impossible to tell potency, without asking.

THE BEST WAYS TO ABUSE A BBS

I HATE PEOPLE WHO CALL ABUSERS HACKERS, IT'S NOT THE SAME THING!!
ABUSERS DO ANYTHING TO MAKE THE BBS A WORSE
THING THEN IT IS AND TO MAKE IT HARDER ON
THIS SYSOP, MOSTLY THE REASONS ARE IS BECAUSE
THE SYSOP IS A MAJOR ASSHOLE. THE FIRST THING IS
TO DISPLAY WHAT TYPE OF THINGS ABUSING STARTS WITH.

1.0 FINDING A BBS TO ABUSE.

TO FIND A BBS TO ABUSE LOOK AT THE BOARD AND THE SYSOP OR USERS, LOOK FOR THESE TYPE OF THINGS,

A, LOOK FOR A SYSOP WHICH TRYS MAKING OUT THAT HIS BBS IS THE BEST AND ALWAYS MAKES MILLIONS OF MESSAGES ON OTHER BOARDS SHOWING WHAT HE'S GOT LIKE "PHONE THE BEST BBS" THEY ARE THE TYPE FO ASSHOLES, GO FOR THEM..

B, LOOK AT THE BBS, IF IT'S A TYPE OF BBS WHICH HAS NOTHING, LIKE THE BBS IS RUNNING ON A 9600 BAUD AND 80 MEG HD BUT HAS LESS FILES THEN WHAT YOU ERASE EACH DAY, THEY SHOULD BE HIT GOOD.

C: GO FOR A BBS WHICH YOU KNOW THAT THE SYSOP THERE DOESN'T KNOW YOU OR YOU NEVER REALLY PHONE THERE, IT'S BETTER FOR NOT BEING CAUGHT, THIS METHOD IS ONLY USED IF YOU ARE GOING TO ABUSE FOR NO REASON OF ALL.

D, FIND A BBS WHICH THE SYSOP HAS A FEW ENERMIES BUT NOT YOU. HE'LL THINK IT'S YOU.

E, FIND A BBS WITH GOOD ACCESS ON FIRST LOG ON, THE TYPE THAT LETS YOU HAVE MESSAGE ACCESS. THEY ARE LOSERS TO ALLOW YOU TO HAVE SUCH ACCESS, UNLESS IT'S A GOOD BBS LIKE THRASHER..

F, FIND A BBS WHICH IS THE MOST HARDEST TO USE, NO ONE LIKES THOSE BOARDS.

G, FIND A BBS WITH A YOUNG SYSOP FROM AGE 13-15, THEY DON'T BOTHER COMPLAINLING TO THE PARENTS ABOUT IT BECAUSE THEY TEND TO SAY, THEN HAVE YOUR LINE OUT, ADULT SYSOPS ARE MOSTLY MORE ASSHOLES. THEY'LL PROBABLY PHONE YOU VOICE TO COMPLAIN..

H, FIND A BBS WHICH PIRATES, THAT WAY YOU CAN SCARE THE HELL OUT OF THEM BY SAYING THINGS LIKE, I'M GOING TO CALL THE COPS. THEY TEND TO FEAR SUCH HASSELMENTS BECAUSE PIRATING IS A MAJOR CRIME.

J, FIND A BBS THAT ALLOWS ALAISES, IT'S HARD TO FIND OUT WHO'S WHO AND IMPOSSIBLE TO VALIDATE PEOPLE. THEY TEND TO GO NON-ALAIS AFTER A

WHILE OF PROBLEMS BUT THEY CAN'T FIGURE OUT WHO'S PRANKING.

K, FIND A BBS WHICH HAS ECHO OR NET MAIL, GET ACCESS TO FULL AREAS,
YOU CAN SCREW ABOUT IN ECHO MAIL AND IT'S HARD TO ERASE IT,
IN TIME IT'LL TRAVEL AROUND THE COUNTRY IF IT'S A WORLD ECHO BASE.

L, FIND A BBS WITH A AREA THAT GIVES YOU ACCESS TO UPLOAD ON FIRST LOG
ON.

M, FIND A SYSOP WHICH DOESN'T VALIDATE USERS.

N, FIND A BBS WHICH IS VERY POPULAR, THE SYSOP TENDS TO HAVE TO MUCH
ON HIS MIND TO VOICE CALL.

O, FIND A BBS WHICH THE SYSOP ISN'T AORUND ALOT,

THOSE ARE SOMETHINGS TO TAKE IN MIND. NOW LETS MOVE INTO
THE GOOD STUFF.

1.1 IF YOU LOG ON, USE A ALAIS, MAKE IT GOOD BUT NOT TO STUPID, NAMES
LIKE "FUCK FUCK" "SHITHEAD" AIN'T GOD ABUSERS, USER SOME OF THE
FOLLOWING.

DR. ABUSER
IT'S_YOUR TURN
THE PUNISHER
THE ABUSER
TOUGH LUCK
FALCON
THE COPS
BOARD ABUSERS
YOUR DEAD
TRASHER MASTER
THE VIRUS
KILLING YOU
RICHARD LITTLE
THE DEIVIL
ABUSE YOU

THOSE AIN'T TOO GOOD BUT YOU GET SOME IDEAS.

1.2 LOG ON, IF YOU GET ON USING THAT TYPE OF NAME THAT I TOLD YOU ABOUT.
IF THE SYSOP IS WATCHING, EITHER THEY'LL HANG UP AND LOCK YOU OUT
OR BREAK IN FOR CHAT, IF THEY BREAK IN FOR A CHAT, HEARS SOME IDEAS
WHICH YOU CAN SAY.

1, I'M BUSY, FUCK OFF
2, I'M GOING TO TRASH YOU BAD!
3, LET ME OUT I HAVE ABUSING TO DO!
4, I HAVE TO CRASH YOUR BOARD NOW, SORRY, UNOIN RULES!
5, CAN I HELP YOU!

6, CAN YOU GIVE ME SYSOP ACCESS
7, WANT TO TRY A NEW VIRUS A MADE.

SURE, MOST OF THOSE ARE SMART REMARKS, BUT YOU CAN'T PLAY DUMB, LET THEM KNOW WHAT YOU ARE UP TOO, IT MAKES THEM EVEN MORE PISSED.

1.3 IF THEY HANG UP, JUST PHONE BACK WITH ANOTHER NAME, IF YOU WANT TO CHAT WITH THEM WHEN YOU PHONE BACK, WHEN IT ASKS FOR YOUR NAME, TYPE THESE:

1, CHAT. I KNOW YOU ARE WATCHING.
2, HELP! THERE'S A KILLER IN MY HOUSE
3, HELLO, THIS ISN'T THAT GUY THAT WAS JUST ON
4, ARE YOU THERE, FUCK OFF
5, DON'T BOTHER ME AND LET ME ON.
6, YOU BBS HANGED UP ON ME! IT'S BROKEN
7, I'M UPLOADING A VIRUS WHICH YOU ARE WATCHING.

THOSE ARE STILL STUPID REMARKS, BUT HEY! THE SYSOP ISN'T PLEASED.

1.4 IF YOU MADE IT ON THE BBS THE FIRST TIME AND THE SYSOP HASN'T NOTICED YOU BECAUSE HE ISN'T AROUND, LOOK AT YOUR ACCESS OPIONS. IF THEY HAVE A BBS LISTER, AND YOU CAN GET IN IT, DO SO.

CHANGE THE NAMES OF THE BBS, SIMPLE DISPLAY.

REALLY NAMES	NOW CHANGED NAMES
Rock Blaster BBS	Bumb blaster BBS
Kings corner BBS	Kings cocker
Jerrys out house	Jerry's house is out
All nite shift	All nite shitting

Bad examples but I'm not thinking at the moment.
Anyways change the sysop names, Number, City and so forth.

1.4 If you want to sit for a few hours, If you have access to a message area, Then toally mess it up, Leave mail to people saying things like this:

1, HOW CAN YOU BE A PART OF THE SHIT BBS
2, AIN'T YOU IN THAT FAG CONTEST
3, FUCK OF, THAT MESSAGE DOESN'T MAKE SENSE
4, GO TO HELL,

If you are able to leave mail using alaises, Look at user or the SysOp's name, Try leaving mail to some one by copying their name with a slight change. LIKE THIS.

FRANK WILLAND -- FRANK WILAND
DON BLUTHE -- DON BLUTH

OR USE THE NAME "THE SYSOP"

LEAVE A MESSAGE LIKE, FUCK OFF, YOU AIN'T WANTED AT THIS BBS.

1.5 THERE ARE TIMES THAT I'VE LOGGED ON A FEW BOARDS WHICH GIVE ONLINE GAMES ACCESS, TRY HANGING UP IN THEM. THAT MAY HANG THE BBS.

1.6 FINALLY, LEAVE MORE THEN 30 PEICES OF MAIL TO THE SYSOP GIVING MESSAGES LIKE.

I'LL BE BACK TO FINISH MY JOB.
YOU AIN'T SEEN THE LAST OF ME.
YOU TERMINATED NEXT TIME.
I'VE TRAHSED ENOUGH OF YOU BBS FOR TODAY.
YOU ARE A FUCKING LOSER!

1.7 PHONE BACK EVERY DAY FOR ABOUT 2 WEEKS, MAKE SURE HE DOESN'T KNOW YOU THAT WELL AND HE'S GOING TO BE PARANOID EVERYTIME SOEONE LOGS ON..

2.0 MOVING TO OTHER WAYS OF ABUSING IS MAKING A GOOD VIRUS, THOUGH I WILL NOT SHOW YOU HOW TO MAKE A VIRUS I'LL GIVE YOU THE BEST WAY TO MAKE SOME ONE RUN IT.

1, FIND A GAME PEOPLE ARE CRAZING FOR, PIRATED MOSTLY.
2, MAKE THE VIRUS AND CHANGE THE NAME TO THE NAME OF THE GAME, MAKE SURE YOU MAKE IT CODED ABIT, LKE DAK.EXE, NOT STREETFIGHTER.EXE, MOST PIRATED GAMES DON'T HAVE THAT.
3, THEN MAKE ABOUT 20 OTHER FILES RELATED TO SUCH A GAME.
4, THEN ZIP THEM UP AND THE VIRUS WILL LOOK LIKE IT'S A ZIPPED GAME AND ONLY YOU WILL KNOW OF IT AS A VIRUS.
5, THEN UPLOAD AND IF THE GAME IS THAT POPLUAR, IT'LL BE DOWNLOADED ALOT WITHIN THE WEEK, EVEN THE SYSOP WILL RUN IT, HE'LL FIRST PORBALBY TAKE IT OFF THE FILE LIST KNOWING IT'S PIRATED THEN TRY IT OUT.

2.1 ANOTHER THING IS TO HAVE MORE THEN 3 OR MORE ACCOUNTS ON A BBS. USE NORMAL NAMES LIKE JASON SMITH, AND GET VALIDATED ON ALL ACCOUNTS, YOU MAY UPLOAD TONS OF VIRUSES TILL THEY FIGURE OUT WHAT'S WRONG, ABOUT 5 ACCOUNTS MAY PUT ABOUT 100 VIRUSES IN A WEEK, AND CRASH LOTS OF COMPUTERS, IT'LL TAKE A WHILE FOR THE SYSOP TO FIGURE OUT THAT ALL UPLOADS CONTAINING THE NAMES OF THE UPLOADERS AND WHEN HE TRYS LOOKING FOR YOU TO ASK IF YOU DID IT INTENDLY, YOU WON'T HAVE YOU REALLY PHONE NUMBER, YOU SHOULD MAKE SURE IT ISN'T YOURS.

2.2 IF YOU GET FULL ACCESS, FIND OUT WHEN THE ECHO MAIL GETS SENT OUT ALL OVER MOST OF THE CITY OF STATE. THEN WRITE MILLIONS OF UNNESSARY MESSAGES ABOUT ALMOST ANY TOPIC, BEST IS TO WRITE ABOUT KNOWN PIRATE BOARDS, THIS WAY IT'LL BE SENT AROUND THE STATE AND POLICE DO READ THESE MESSAGES AND SO OR LATER THERE'LL BE MAJOR PROBLEM.

2.3 ALSO, IT'S HARD BUT THERE MAYBE A TIME TO GET AHOLD OF SOMEONES PWORD. TRY FINDING SOMEONE WHO YOU KNOW AND ASK FOR THE USER LIST AND PWORDS.

AND THEN USE THEM ON OTHER BOARDS, MOST PEOPEL STICK WITH THE SAME
PASSWORD. YOU CAN DO ALMOST ANYTHING FROM POSTIN ECHO MESSAGES, UPLOADING
VIRUSES AND ABUSING THE BBS.

2.4 WRITE MESSAGES ON THIGNS THAT CAN REFLICT MANY PEOPLE, SAY THAT THERE'S
A VIRUS WITH A TYPE OF TIME BOMB ON IT, IT'LL GO OF WITHIN 2 MONTHS
AND THE VIRUS STARTED ON A BBS FILE AREA AND MOST FILES FORM THAT BBS
ARE INFECTED. IT'LL TURN HEADS REALLY FAST, ALSO POST MESSAGES LIKE
THERE'S A RUMOUR THAT A SYSOP ON ANOTHER BBS IS RUNNING AN ABUSING SECTION
AND HAS OVER 200 ZIP UP VIRUSES THAT RUN BY THE .EXE, IT'LL AGAIN CAUSE
PROBLEM...

2.5 TRY LOADING A GAME AND TYPING A CODE LIKE "[2][/4][SHELL][TO][DOS]
IF THE SYSOP IS WATCHING YOU MAY THINK YOU KNOW SOMETIHNG BAD!

What You Should Know About Collection Agencies

Karen Hartney laughed when she pulled the lavishly illustrated book on Galapagos Islands wildflowers out of her mailbox. She hadn't ordered thebook, wasn't about to pay for it, and felt no obligation to go to thetrouble and expense of returning it. Two weeks later, she was billed $29.95, plus mailing and handling. Shethrew the statement in the trash. In time, the letters grew nasty,demanding payment and warning that her credit rating would suffer if shedidn't respond promptly. When a collection agent began calling her at work,she snapped. "Leave me alone," Karen hissed. "I never wanted that dumb bookanyway!" "You might have thought of that before you decided to keep it," the manresponded. "I think the word for taking things that aren't yours is'stealing.'" Karen (whose name has been changed) was furious-- but also worried.Could the collection agency harm her credit rating, contact her employer,neighbors, landlord? Most of al
l, she just wanted the harassing calls andletters to stop. Though resentful, she mailed the payment-- now a full$37.50, including interest and collection charges. Karen's case is not an isolated one. Despite the strong new consumerprotection laws passed in recent years, abuses still exist, and a sizeableminority of retailers and collection agencies engage in such illegalcollection practices. Charging for unordered goods is only one of the manyactivities that are prohibited by federal law. (If, by the way, you receiveunrequested merchandise as Karen did, you are under no obligation to pay.You may treat it as a free gift, but you should notify the sender, inwriting, of your intention as soon as you receive a "bill".) The thorniest problems occur when a debt is truly owed and a consumer,through overextension or inadvertence, falls behind in paying it. In thiscase, the account is often turned over to a collection agency, which maybehave unethically in i
ts effort to recoup the money. "Some of the most extreme cases we see involve actual threats ofviolence," reports Diane Conner, staff attorney for the Credit PracticesDivision of the Federal Trade Commission (FTC). "Children have been toldover the phone, 'Tell your parents they're going to jail tomorrow if wedon't get the money.' We've also heard about collection agencies trying toadd on illegal fees of up to 100 percent of the original debt." Federal law protects you against such abusive practices. By knowingwhich tactics are illegal and how to stop them, you can avoid being avictum.BEYOND THE LEGAL LIMIT____ The following are violations of consumer protection laws: REPETITIVE CALLING OR CALLS AT UNUSUAL TIMES OR PLACES. Some collectionagents will call a consumer repeatedly during a single day, or telephonelate at night without permission-- both of which are clearly illegal underthe Fair Debt Col

lection Practices Act (FDCPA). Calls at work are not considered "harassing" if an office is the mostconvenient place for you to receive the call-- but, says Diane Conner, "If the agent knows that your employer does not allow you to receive personalcalls at work, or if you've asked not to be contacted there, then it wouldbe a violation." CALLS TO PERSONS OTHER THAN THE CONSUMER. If a collection agent hasbusiness with you, you are the only person with whom he may discuss thatbusiness. "We frequently hear that a collection agent has called anemployer, or perhaps a neighbor, and left an "urgent message' that theconsumer should call XYZ Collection Agency regarding payment of a debt,"reports Bill McDonough, an FTC staff attorney. "The only motive would be toembarass the consumer, and it's against the law." ABUSIVE, OBSCENE, OR THREATENING LANGUAGE. Late bill payers have beencalled deadbeats and bums, subjected to rude and obscene language, and givenveiled as well as direct threats of violence and imprisonment. If thishappens, end the conversation immediately, requesting that you never becontacted again. Follow up with a brief letter barring future contact withthe collection agency. You may then wish to file a complaint with the FTCor state consumer protection agency, or pursue private legal action. MISLEADING THREATS OF LEGAL ACTION. No one has the right to make falsethreats or to claim that legal action has been or is about to be institutedif that's not the case. Also prohibited are papers that look like officialnotices from a state agency or court of law-- including documents withheadings that mimic a common legal form (such as "Ace Collection Agency v.Jane Consumer") or ones that use an agency name similar to that of a state orfederal agency. OTHER ABUSIVE BEHAVIOR. Because debt collectors show infiniteingenuity, the Fair Debt Collection Practices Act covers scores of otherforbidden tricks, from tacking on collection charges not authorized bycontract or law, to using false names and publishing lists of consumers indebt. Realizing that it could not forsee every possible abuse, Congresseven added a prohibition against any "harassing, oppressive, and abusiveconduct"-- a general phrase that increases the power of the courts and theFederal Trade Commission to protect you against improper collectionpractices.STEPS TOWARD SELF-DEFENSE____ What can you do if you're the victum of an overeager collection agency?Your first and simplest option under the FDCPA is to request in writing thatall collection contacts stop. Once you do that, the collection agency isnot allowed to call or write to demand payment; it can only advise you ofnew action, such as the referring of your account back to the creditor orthe filing of legal action. if the harassment continues, you may wish to contact your stateconsumer agency.

According to Cyra Narva of the Consumer AssistanceDivision of the Massachusetts State Banking Department, these agencies willoften intervene to solve the problem. "Usually," Narva reports, "theconsumer is content just to know that the rug has been pulled out from underthe collection agency and that the abusive practices will stop." The agencies won't compensate you for their past harassment; however asuccessful lawsuit might. You could bring suit under the FDCPA and, ifsuccessful, recover a cash judgement of actual damages suffered, attorney'sfees, sourt costs, and a special statutory award of up to one thousanddollars. "If a consumer has been truly injured," says Willard Ogburn, deputydirector of the National Consumer Law Center, "he or she is entitled to becompensated. The fact that attorney's fees may be recovered in a successfulcase encourages some attorneys to pursue strong cases on a commission basis,while the possibility of an extra statutory award of up to a thousanddollars acts as an extra incentive to the consumer. Meanwhile, the publicinterest is served as collection agencies learn that violating consumerprotection laws can be very expensive." Whatever decision you make, you're sure to reap some gratification fromsimply standing up for your rights and the rights of others like you.Rudeness and abuse need never be tolerated, and you can see to it that they're not

STOPPING TROUBLE : CONSUMER AGENCIES THAT CAN || BEFORE IT STARTS | | HELP YOU PROTECT YOURSELF || | | || Healthy credit use is not | | THE FEDERAL TRADE COMMISSION || inconsistent with sound | | (FTC). Your regional office || personal finance management, | | can advise you of your rights || but if you overextend, these | | and may even make an investi- || measures should enable you to | | gation if a collection agency's || resolve the problem without | | abuse has been severe or if || becoming vulnerable to further | | yours is one of several com- || embarassment or harassment: | | plaints against the same || | | agency. Meanwhile, let both || IMMEDIATELY

```
CONTEST IN WRITING |   | creditor and collection  agency  ||  ANY  INACCURATE  CHARGES,
AND  |    |  know th
at  you've  alerted  the  ||  REQUEST VERIFICATION.          |    | FTC.  Their attitudes  may  not  ||  No
collection  activities  may  |    |  improve,   but  their  behavior  ||  proceed   until  a  charge  is  |    |  probably
will.                  ||  verified:   Waiting may make a  |    |                              ||  challenge more difficult.       |
|  STATE    CONSUMER    PROTECTION  ||                              |    |  AGENCY.   In some states,  this  ||
IF YOU REALIZE  THAT  YOU  ARE  |    |  government office can arbitrate  ||  NOT GOING TO BE
ABLE  TO  MAKE  |    |  a  dispute   and   order   that  ||  REQUIRED PAYMENTS ON  A  DEBT,  |    |
abusive practices  be  stopped.  ||  CONTACT THE CREDITOR.     Most  |    |  If your debt is  undisputed
or  ||  are  understanding   and   co-  |    |  can be proved,  the agency  can  ||  operative if  you  propose  an  |
|  help you negotiate a reasonable  ||  alternate payment plan at  the  |    |  extended-payment plan;  it  may
  ||  first sign of trouble.  Review  |    |  also  have  greater   power  to  ||  your own budget,  determine  a  |    |
intervene in an individual case  ||  monthly amount you can  afford  |    |  than  a  regional  FTC   office  ||  to
pay,   then  explain   the  |    |  would.                         ||  problem to  the  creditor  and  |    |   To learn what
state  services  ||  offer  to   pay   the   lesser  |    |  are available  to  protect  you  ||  amount.                     |
|  against collection  harassment,  ||                              |    |  contact your  state  government  ||  DON'T
ALLOW YOUR ACCOUNT TO BE  |    |  information-office   or    your  ||  TRANSFERRED  TO  A
COLLECTION  |    |  state    attorney    general's  ||  AGENCY    THROUGH    YOUR    OWN  |    |  office.
||  INACTION.     Creditors     use  |    |                              ||  collection  agencies  to  goad  |    |    If the
improper conduct comes  ||  the  reluctant  or
  forgetful.  |    |  from an attorney practicing law  ||  A  creditor  who   understands  |    |  in the collection
area, contact  ||  that you are overextended  but  |    |  your LOCAL BAR ASSOCIATION, and  ||  doing the
best  you  can  will  |    |  ask for the disciplinary  board  ||  have no reason  to  resort  to  |    |  or   licensing
agency    that  ||  such measures.                 |    |  receives   complaints   against  ||    Many people are too
anxious  |    |  lawyers.   They probably  won't  ||  or embarassed  to  approach  a  |    |  step in  directly;
however,  a  ||  creditor  about  dificulty  in  |    |  lawyer    who    knows    that  a  ||  making payments.
Remember that  |    |  complaint   is  being   checked  ||  the creditor, whether a merch-  |    |  generally takes
more  care  to  ||  ant or a banker, wants to keep  |    |  act within  legal  and  ethical  ||  your  business.   An
amicable  |    |  bounds.                       ||  resolution is in  "everyone's"  |    |
                              ||  interest.                   |    |  CONSUMER   CREDIT    COUNCELING  ||
|    |  AGENCIES.     Frequently    the  |+----------------------------------+    |  problem is less one of outright  |
|  harassment than of anxiety  and  |                                  |  increasingly short  tempers  on  |
|  both sides.   A nonprofit  con-  |                                  |  sumer credit counceling  agency  |
|  has  no  official   enforcement  |                                  |  power, but it  "can"  help  you  |
|  assess your financial situation  |                                  |  and act as a mediator in making  |
|  more mutually suitable  payment  |                                  |  arrangements.
      |                                  |                              |
```

HEY THERE KARDERS!! MANY OF MAY NOTKNOW THAT IT IS POSSIBLE TO SEND MONEY VIA WESTERN UNION AND CHARGEIT TO A KREDIT KARD. THE MONEY IS THEN PICKED UP AT ANYWESTERN UNION OFFICE. THE MONEY HASTO BE SENT AT LEAST 50 MILES FROMWHERE YOU ARE CALLING. WESTERN UNION WILL WANT TO CALL YOUBACK TO VERIFY YOUR #. THEY DO NOTHAVE ACCESS TO THE KARD HOLDERSREAL WORK # AND IF THEY DID YOUCOULD SAY YOU DONT WORK THERE ANYMORE. THERE ARE 3 WAYS TO DO THIS 1 USE A LOOP (MAY NOT WORK) 2 GOTO KARD HOLDERS RESIDENCE ANDTAP ONTO THERE LINE. BE SURE TODISSCONNECT CUST SIDE. 3 GOTO ANY BUISNESS AND USE THERELINE AND SAY YOU WORK THERE. BE URE TODISSCONNECT CUST SIDE. AFTER WESTERN UNION CALLS YOU BACKYOU WILL NEED TO PROVIDE THE FOLLOWINGINFO. CARD #NAME ADDHOME #WORK #EXP DATEISSUING BANK IF THE MONEY ORDER IS A LARGE AMOUNTYOU ....MIGHT...BE REQUIRED TO PROVIDETHIS ADDITIONAL INFORMATION. SS#DATE OF BIRTHBANK BRANCH (TOWN)FIRST BORN CHILD (JUST

KIDDING) AS YOU CAN SEE THIS IS NOT FOR THEWEEK HEARTED. ITS BEST TO HAVE THEMONEY W
IRED TO A CHECK CASHINGPLACE THATS ON THE WESTERN UNIONNETWORK. THEY WILL BE ABLE TO GIVEYOU CASH ON THE SPOT WITH OUT ID. THE MONEY ORDER AMOUNT CANNOT EXCENDTO CASH ADVANCE LIMIT SET BY THEBANK. IF SOMEONE IS HOME AT THE CARD HOLDERSRESIDENCE DURING THE TRANSACTION YOUSHOULD DISSCONNECT THEIR PHONE. THISWILL PREVENT THEM FROM VERIFING. IF YOURE MISSING A FEW OF THE FACTSYOU CAN TRY CALLING THE ISSUINGBANK AND ASKING THEM. IF YOU KNOWCARD # NAME AND PH# THEY WILLUSUALLY TELL YOU WHAT YOU WANT TO KNOW. ISSUING BANK CAN BE FOUND OUT BYCALLING 800-228-1122 ASK FOR MERCHANTINFO. ASK FOR ISSUING BANK USE THEMERCHANT # 541-388-0084-50512. THEFIRST 6 DIGITS OF THE CARD ARE THEISSUING BANKS #. OH YEA..WESTERN UNION 800-325-6000ASK FOR MONEY ORDERS HAPPY KARDING!!! DONT PHUCK UP!!!GETS YOUR FACTS STRAIGHT FIRST!!!

* PRIVATE AUDIENCE *   (A BASIC LESSON IN THE ART OF LISTENING IN)
=-

PART I: THE LAWw: Section 605 of tital 47 of the U.S code, forbids interceptionof communication, or divulagance of intercepted communicationexept by persons outlined in section 119 of tital 18 (a portionof the Omnibus crime controll and safe streets act of 1968).This act states that "It shall not be unlawfull under this actfor an operator of a switchboard, or an officer, employe, oragent of any communication common carrier who's switching systemis used in the transmision of a wire communication to interceptor disclose intercepted communication."hat all this legal bullshit is saying is that if you don't workfor a phone company then you cant go around tapping people'slines. If you decide to anyway, and get caught, it could cost youup to 5 years of your life and $10,000. This, you are allassuming means that if you tap someone eles's line, you will bepunished....wrong! You can't tap your own line either. Thepunishment for this is probably no more than a slap on the hand,that is if they act
ually catch you, but it's a good thing toknow.............now on to the fun.....   PART II: TAPPINGverone has at sometime wanted to hear what a friend, theprincipal, the prom queen, or a nighbor has to say on the phone.There are several easy ways to tap into a phone line. None of themethods that I present will involve actully entering the house.You can do everything from the backyard. I will discuss fourmethods of tapping a line. They go in order of increasingdifficulty.1. The " beige box ": a beige box (or bud box) is actually betterknown as a "lineman" phone. They are terribly simple toconstruct, and are basically the easiest method to use. Theyconsist of nothing more than a phone with the modualr plug thatgoes into the wall cut off, and two alligator clips attached tothe red and green wires. The way to use this box, is to ventureinto the yard of the person you want to tap, and put it onto hisline. This is best done at the bell phone box that is usuallynext to the gas meter. It should on
ly have one screw holding itshut, and is very easily opened. Once you are in, you should see4 screws with wires attached to them. If the house has one line,then clip the red lead to the first screw, and the green to thesecond. you are then on the "tappie's" phone. You will hear anyconversation going on. I strongly recomend that you remove thespeaker from the phone that your using so the "tappie" can'thear evcery sound you make. If the house has two lines, then thesecond line is on screws three and four. If you connecteverything right, but you dont get on the line, then you probablyhave the wire's backward. Swich the red to the second screw andthe green to the first. If no conversation is going on, you mayrealize that you cant tap the phone very well because you don'twant to sit there all night, and if you are on the phone, thenthe poor tappie can't dial out, and that could be bad...so.......method two.2. The recorer: This method is probably the most widespread, andyou still don't have to be a genius to do it.
There are LOTS ofways to tape conversations. The two easiest are either to put a"telephone induction pickup" (radio shack $1.99) on the biege boxyou were using, then pluging it into the microphone jack of asmall tape recoder, and leaving it on record. Or pluging therecorder right into the line. This can be done by taking awalkman plug, and cutting off the earphones, then pick one of thetwo earphone wires, and strip it.

There should be another wireinside the one you just stripped. Strip that one too, and attachaligators to them. Then follow the biege box instructions to tapethe conversation. In order to save tape, you may want to use avoice activated recorder (Radio shack $59), or if your recorderhas a "remote" jack, you can get a "telephone recorder control"at Radio shack shack for $19 that turns the recorder on when thephone is on, and off when the phone is off. This little box plugsright into the wall (modularly of course), so it is best NOT toremove the modular plug for it. Work around it if you can. Ifnot
, then just do you best to get a good connection. Whenrecording, it is good to keep your recorder hidden from sight (inthe bell box if possible), but in a place easy enough to changetapes from. The wireless microphone: this is the BUG. It transmitts asignal from the phone to the radio (Fm band). You may remember Mrmicrophone (from kaytel fame), these wireless mirophones areavailible from radio shack for $19. They are easy to build andeasy to hook up. There are so many differant models, that is isalmost imposible to tell you exactly what to do. The most commonthing to do, is to cut off the microphone element, and attachthese two wires to screws one and two. the line MIGHT, dependingon the brand, be "permenently off hook" this is bad, but byphucking around with it for a while, you should get it working.There are two drawbacks to using this method. One, is that thepoor asshole who is getting his phone tapped might hear himselfon "FM 88, the principal connnection". The second problem is therange. The store bought transmitters have a VERY short range. Isuggest that you build the costomized version I will present inpart four (it's cheaper too). Now on to the best of all themethods....4. The "easy-talks": This method combines all the best aspects ofall the the other methods. It only has one drawback... You need aset of "Easy-tylk" walkie talkies. They are voice activated, andcost about $59. You can find em at toystores, and "hi-tech"catalogs. I think that any voice activated walkie talkies willwork, but I have only tried the easy-talks. First, you have todecide on one for the "tramsmitter" and one for the "reciever".It is best to use the one with the strongest transmition totrasmitt, even though it may recieve better also. Desolder thespeaker of the "transmitter", and the microphone of the"reciever". now, go to the box. put the walkie talkie on "VOX"and hook the microphone leads (as in method three) to the firstand second screws in the box. Now go home, and listen on yourwalkie talkie. if nothing happens, then the phone s
ignal wasn'tstrong enough to "activate" the transmission. If this happensthere are two things you can do. One, add some ground lines tothe microphone plugs. This is the most inconspicuous, but if itdesn't work then you need an amplifier, like a walkman with twoearphone plugs. Put the first plug on the line, and then into oneof the jacks. Then turn the voulume all the way up (w/outpressing play). Next connect the second earphone plug to the micewires, and into the second earphone outlet on the walkman. nowput the whole mess in the box, and lock it up. This should do thetrick. It gives you a private radio station to listen to them on,you can turn it off when something boring comes on, and you cantape off the walkie talkie speaker that you have!   PART IV: WIRELESS TRANSMITTER PLANZis is a tiny transmitter that consists on a one colpittsoscillator that derives it's power from the phone line. Since theit puts on the line is less than 100 ohms, it has noeffect on the telephone performance, and can not
be detected bythe phone company, or the tappie. Since it is a low-powereddevice using no antenna for radiation, it is legal to the FCC.(That is it complies with part 15 of the FCC rules andregulations). It, however is still illeagal to do, it's just thatwhat your using to do it is legal. This is explained later inpart 15... "no person shall use such a device for evesdroppingunless authorized by all parties of the conversation" (then it'snot evesdropping is it?). What this thing does,is use four diodesto form a "bridge rectifier". It produces a varying dc voltagevarieng with the auto-signals on the line. That voltage is usedto supply the the voltage for the oscillator transistor. Which isconected to a radio circuit. From there, you can tune it to anyzhannel you want. The rest will all be explianed in a minute....PARTS LISTem | description---C1 | 47-Pf ceramic disk capaciterC2,C3 | 27-Pf mica
capaciterCR1,CR2,CR3,CR4 | germanium diode 1n90 or equivalentR1 | 100 ohm, 1/4 watt 10% composition resistorR2 | 10k, 1/4 watt 10% composition resistorR3 | .7k, 1/4 watt 10% composition resistorL1 | 2 uH radio frequency choke (see text)L2 | 5 turns No.20 wire (see text)Q1 | Npn rf transistor 2N5179 or equivalent---1 may be constructed by winding approximately 40 turns of No. 36enamal wire on a megohm, 1/2 watt resistor. The value of L1 isnot critical. L2 can be made by wrapping 5 turns of No. 20 wirearound a 1/4 inch form. After the wire is wrapped, the form canbe removed. Just solder it into place on the circuit board. Itshould hold quite nicely. Also be sure to position Q1 so that theEmmiter, Base, and collector are in

the proper holes. Theschmatic should be pretty easy to follow. Although it has anunusual number of grounds, it still works.

```
           |------------------L1----------------|              --                            |          CR1 /  \ CR2            |---
-------------|A--------------/    \ --|        ----|        |    |      |      \    /   |        |  |        C2    L2      |    CR3 \
/CR4 |        C1  R2    |----|     |      R1        --     |        |  |   gnd   C3    |       |        |     |        ----|        |-----|
|       gnd     |            |             |      |             |           |-----|----Base  collector      |             |
R3     \   /B-----------------------|                |      \/\ <- Q1                                  gnd       \/
|                                    |                                    emmitter(gnd)e odd thing about this bug
```

that we havent encountered yet, isthat is is put on only one wire (either red or green)
so go tothe box, remove the red wire that was ALREADY on screw #1 andattack it to wire 'A' of the bug then attach wire 'B' to thescrew itself. you can adjust the frequency which it comes out on(the Fm channel by either smooshing, or widening the coils of L2.It takes a few minutes to get to work right, but it is also veryersatile. You can change the frequency at will, and you caneasily record off your radio.
PART FIVE: HELPFULL HINTSFirst of all, With method one, the beige box, you may notice thatyou can also dial out on the phone you use. I don't recomend thatyou do this. If you decide to anyway, and do somethingconspicuous like set up a 30 person conferance for three hours,then I suggest that you make sure the people are either out oftown or dead. In general when you tap a line, you must becarefull. I test everything I make on my line first, then installit late at night. I would not recoment that you leave a recorderon all day. Put it on when you want it going, and take it offwhen your done.
As far as recording goes, I think that if thereis a recorder on the line it sends a sporatic beep back to thephone co. I know that if you don't record directly off the line(i.e off your radio) then even the most sophisticated equipmentcan't ell that your recording. Also, make sure that when youinstall something the people are NOT on the line. Installationtends to make lots of scrachy sounds, clics and static. It isgenerally a good thing to avoid. It doesn't take too muchintelligence to just make a call to the house before you go toinstall the thing. If it's busy then wait a while. (This ofcourse does not apply if you are making a "midnight run").All in all, if you use common sense, and are *VERY* Carefull,chances are you wont get cought. Never think that yourunstopable, and don't braodcast what your doing. Keep it toyourself, and you can have a great time.   -[OVERLORD]-The CircleLordTARAN KINGight Lightninghe Forest Ranger-80 systemswatch for more advanced tapping, how they catch you, and
verification in the near future.

"WIRETAPPING, BUGS ON LINES AND LISTENING IN."

Many phreaks are not very knowledgeable when it comes to wiretapping, bugs,and parties listening in on ones line. For those of you who know a lot aboutwiretaps and etc. then this file may seem out of place. Although many phreaks think of legal wiretaps as the most common way for thephone company to check your calling activity, there are others. Under court order, the phone company may attach a "Pen Register" to your phone wires at thecentral office. The device gives a printout of all calls, local and long distance, going out of your phone including time of day, duration of call, and,of course, the recipient's number. It's used mostly by law enforcement agenciesto check who you are calling in hopes that the other party will shed some lighton your alleged wrongdoing. Law enforcement agencies often prefer the Pen Register to an out-and-out wiretap. It takes lesr work, less manpower (the Pen Register is automatic; thegumshoes just come by the phone company and pick up the printout), and less hassle to obtain a
court order for its installation, because it's less of aninvasion of privacy than a wiretap. HOW WIRETAPPING WORKS. Listening to phone calls isn't very difficult to do,although it is clearly illegal. The quickest method wiretappers use is simplyto cut into someone's phone line, preferably where the owner can't detect it(near the garage or behind the pole, for example) and wire in their own head-set. Then they remove the mouthpiece, so the person being tapped can't detectthe wiretapper's breathing or other noise. If a wiretapper can't stick around,he'll use a high-impedance coupling transformer and feed the wire into a taperecorder.   To save tape, most tappers use the type of recorder that records automticallywhen it hears a voice. Another procedure is to find the right "pair." That's telephone-tapping talk for the two wires that go

into your house and that ofothers in your building or apartment. The boxes that contain pair terminals arecalled terminal boxes and can usually be found in basements of apartment
s oroffice buildings, or occasionally on the outside wall of a building. A wiretapper typically will have an accomplice call the number being tapped.That puts about 90 volts on the line. The tapper takes two fingers and run themdown the rows terminal. When he hits the right phone pair, he feels a jolt. Once he's found it, he's got the right phone; a listening device is then attached. For those who prefer the wireless approach, a "bug" placed in a phone willtransmit conversations over short distances. Bugs come in all sizes shapes.A cheap type sometimes goes by the name of "Wireless Microphone." Let's face it; it's a bug. Anyone can buy them at Radio Shack or even some toy stores forless than $15. It's range is limited, usually 500 to 1,000 feet, but it will fit inside a phone and send a clear signal to an FM radio. Or better yet, it ispossible to connect the wireless mike through a high impedance transformerconnected to the phone line, and no one has to enter the tapee's house. A wiretapper also can buy bug
s that look like telephone mouthpieces. They'reinserted by unscrewing the mouthpiece and replacing it with a souped-up version. COURT-AUTHORIZED WIRETAPS INSTALLED, 1979.New
Jersey..........................144 Virginia.............................5New York...........................118 District of
Columbia.................3Florida.............................63
Nevada...............................2Maryland............................23
Hawaii...............................2Massachusetts.......................22 Rhode
Island..........................2Nebraska............................21
Delaware.............................2Connecticut.........................15 New
Mexico...........................1Arizona.............................12
Oregon...............................1Georgia.............................10 LISTENING IN. If you own a scanner radio to listen in on police and fire calls, you can check up on your local phone company repair trucks, installers,and lineman, too. Although the
 radio channels phone companies use vary fromarea to area, most are assigned one or two of the following frequencies: 151.34, 451.175 - 451.275, 451.3 - 451.675, 456.175, 456.275 (mobile), 456.300 - 456.675 (mobile), 462.475, 462.525, 467.475 (mobile), 467.525 (mobile). Also,if you want to eavesdrop on callers using conventional mobile phone service, try these frequencies: 158.07 - 158.49 for mobiles and 152.81 - 153.03 for basestations. (All frequencies are in MegaHertz, or MHz.)Remember: It's against thelaw to divulge the contents of any conversations you may hear, but it's okay tolisten. JUST LISTEN FOR THE BEEP. When can you legally tape a conversation off the phone? It's certainly easy enough to do; it can be accomplished with use of atwo-dollar suction cup device, as well as with most models of answering machines.A-uhe Federal Communications Commision fequires phone compaines to includeinformation in their tariffs outling what is acceptable, and enforcement is left to each local phone company. State l
aws differ, but the rule of thumb is that a short beep heard every 15seconds indicates that the person on other end is recording the conversation.In some states, mutual consent can substitute for the beep tone; you need onlyask permission of the other party, and the taping is perfectly legal. Of course, the technology has made it virtually impossible in some cases to detect whether someone is taping (it's easy enough to have a tape recorder going in aroom with your speakerphone, and even the most sophisticated devices won't beable to tell the difference), but the penalities for taping your own conversations are minimal. If you are caught, which is difficult in itself, thepenalty "MAY" be suspension of phone service. Third-party wiretapping -- taping a conversation of which you are not a part is another story. This is an area in which the federal government takes agreat intrest. Quite simply, it's a crime under federal and state laws to intercept calls unless you happen to be a party to the conversation or unl
essyou first obtained the consent of one of the parties taking part in the call.Law enforcement offficals can listen in on your conversations after having secured the proper court order, but you have to be a hot number to warrant thatsort of attention. If you do decide to listen in on your suspected-of-cheatingspouse (and the equipment to do it with is not too difficult to come by), beforwarned that for your troubles, you could get five years behind bars and a$10,000 fine. Remember wiretapping can be granted by any federal judge. Many phreaksalways complain about their line being wiretapped well hopefully the fileabove has taken care of that.

Introduction
============

The Lunch Box is a VERY simple transmitter which can be handy for all sorts of things. It is quite small and can easily be put in a number of places. I have successfully used it for tapping fones, getting inside info, blackmail and other such things. The possibilities are endless. I will also include the plans for an equally small receiver for your newly made toy. Use it for just about anything. You can also make the transmitter and receiver together in one box and use it as a walkie talkie.

Materials you will need
=======================

(1) 9 volt battery with battery clip
(1) 25-mfd, 15 volt electrolytic capacitor
(2) .0047 mfd capacitors
(1) .022 mfd capacitor
(1) 51 pf capacitor
(1) 365 pf variable capacitor
(1) Transistor antenna coil
(1) 2N366 transistor
(1) 2N464 transistor
(1) 100k resistor
(1) 5.6k resistor
(1) 10k resistor
(1) 2meg potentiometer with SPST switch
Some good wire, solder, soldering iron, board to put it on, box (optional)

Schematic for The Lunch Box
===========================

This may get a tad confusing but just print it out and pay attention.

```
      [!]
       !
      51 pf
       !
    ---+----  ------------base   collector
   !       )(            2N366       +----+------/\/\/----GND
  365 pf     ()            emitter          !
   !       )(               !           !
   +--------  ---+----        !            !
   !           !    !       !           !
  GND          /  .022mfd    !            !
           10k\    !       !           !
              /   GND      +-----------------------emitter
              !          !           !          2N464
              /         .0047          !         base   collector
          2meg  \----+       !            !   +--------+      !
              /    !      GND           !   !              !
                 GND                    !   !              !
  +-------------+.0047+--------------------+   !              !
                                     !   +--25mfd-----+
     -----------------------------------------+   !          !
 microphone                                  +--/\/\/-----+
     ----------------------------------------------+   100k    !
                                                !
         GND---->/<---------------------!+!+!+---------------+
             switch                Battery
           from 2meg pot.
```

Notes about the schematic
========================

1. GND means ground
2. The GND near the switch and the GND by the 2meg potentiometer should be connected
3. Where you see:)(

```
                  ()
                  )( it is the transistor antenna coil with 15 turns of
                     regular hook-up wire around it.
```

4. The middle of the loop on the left side (the left of "()") you should run a wire down to the "+" which has nothing attached to it. There is a .0047 capacitor on the correct piece of wire.
5. For the microphone use a magnetic earphone (1k to 2k).
6. Where you see "[!]" is the antenna. Use about 8 feet of wire to broadcast approx 300ft. Part 15 of the FCC rules and regulation says you can't broadcast over 300 feet without a license. (Hahaha). Use more wire for an antenna for longer distances. (Attach it to the black wire on the fone line for about a 250 foot antenna!)

Operation of the Lunch Box
=========================

This transmitter will send the signals over the AM radio band. You use the variable capacitor to adjust what freq. you want to use. Find a good unused freq. down at the lower end of the scale and you're set. Use the 2 meg pot. to adjust gain. Just fuck with it until you get what sounds good. The switch on the 2meg is for turning the Lunch Box on and off. When everything is adjusted, turn on an AM radio adjust it to where you think the signal is. Have a friend say some shit thru the Box and tune in to it. That's all there is to it. The plans for a simple receiver are shown below:

The Lunch Box receiver
=====================

(1) 9 volt battery with battery clip
(1) 365 pf variable capacitor
(1) 51 pf capacitor
(1) 1N38B diode
(1) Transistor antenna coil
(1) 2N366 transistor
(1) SPST toggle switch
(1) 1k to 2k magnetic earphone

Schematic for receiver
=====================

```
        [!]
         !
        51 pf
         !
    +----+----+
    !         !
    )       365 pf
    (----+    !
    )    !    !
    +---------+---GND
         !
         +---*>!----base  collector-----
           diode      2N366          earphone
                   emitter    +-----
                     !        !
                    GND       !
                              -
                              +
                              - battery
                              +
          GND------>/<------------+
                switch
```

Closeing statement
=================

This two devices can be built for under a total of $10.00. Not too bad. Using these devices in illegal ways is your option. If you get caught, I accept NO responsibility for your actions. This can be alot of fun if used correctly. Hook it up to the red wire (I think) on the fone line and it will send the conversation over the air waves.

NITROUS OXIDE------------- THE PREPARATION FOR NITROUS OXIDE IS SO EASY, THAT MOST READERS WILL PROBABLYNOT BELIEVE ME. NITROUS OXIDE IS A COLORLESS GAS, WHICH IS SLIGHTLY SOLUBLE INWATER. THE NAME 'LAUGHING GAS' COMES FROM THE FACT THAT IT CAUSES A SLIGHT HYSTERIA IF INHALED. IT IS DENSER THAN AIR, AND HAS ANASTHETIC-LIKE EFFECTS,INADDITION TO HYSTERIA. IT WAS USED AS A DENTAL ANASTHETIC FOR A FEW YEARS, BUTCOMPOUNDS WERE MADE THAT DID THE SAME JOB, BUT WITHOUT THE SIDE EFFECT. IT ISSOMETIMES USED TO BOOST ENGINES TEMPORARILY, BUT I WOULDN'T KNOW ABOUT THAT TYPE OF THING. I DO KNOW THAT UNLESS YOU KNOW EXACTLY WHAT YOU ARE DOING, THEBOOSTING PROCESS IS EXTREMELY DANGEROUS AND EXTREMELY DAMAGING TO THE ENGINE.. I DO NOT SUGGEST THAT YOU JUST PRESSURIZE THE STUFF, AND SEND BURSTS OF IT TO YOUR ENGINE.MATERIALS:----------10 GRAMS OF AMMONIUM NITRATETESTUBE OR ERLENMYER FLASKRUBBER STOPPER W/HOLE FOR TUBING3 INCH GLASS TUBEAPPX 24 INCHES RUBBER TUBEBOTTLE, LARGEFILTER MASK OR GAS MASK(OPTIONAL)TWO PIECES OF WOOD, OF A SIZE TO FIT INSIDE THE PAN WITH ABOUT A ONE INCH SPACE IN BETWEEN THE WOOD. APPX1 1/2 TO 1 INCH THICK.SOURCE OF FLAMECLAMP, FOR TEST

TUBETAPE (ELECTRICAL)GLASS PLATE AS WIDE AND LONG AS THE MOUTH OF THE BOTTLEPROCEDURE:---------- 1. PLACE THE AMMONIUM NITRATE INSIDE THE TEST TUBE. LEAVE LOOSE, AND MAKESURE THAT IT WILL NOT BE UNDER SEVERE PRESSURE. 2. NOW, PLACE THE GLASS TUBE ALL THE EAY THROUGH THE STOPPER. IT MUST BEALL THE WAY THROUGH: ******* ******* ++++++++++++++ ******* ********=RUBBER, +=TUBE THIS IS SO THAT THE RUBBER WILL NOT CLOSE OFF ON THE INSIDE, AND THE RESULTING PRESSURE DOES NOT SHOOT THE TOP OFF!!!!!!!! 3. PLACE THE STOPPER INSIDE THE TEST TUBE. PLACE ONE END OF THE RUBBER TUBINGON THE PROJECTING END OF THE GLASS TUBE. TAPE THE CONNECTION TIGHTLY, SO THATTHERE IS NO LEAKAGE. 4. NOW, PLACE THE TWO BOARDS IN THE PAN LIKE SHOWN: *********** *++++ ++++* *++++ ++++* *++++ ++++* *++++ ++++* *++++ ++++* *********** +=WOOD, *= PAN RIM. THE SPACE IN THE CENTER IS WHERE THE RUBBER TUBING WILL GO. 5. FILL THE PAN WITH WATER SO THAT IT RISES APPX. 1/2 INCH ABOVE THE SPACEIN THE CENTER. 6. FILL THE BOTTLE WITH WATER AS CLOSE TO THE TOP AS YOU CAN. PLACE THE GLASSPLATE OVER THE TOP OF THE BOTTLE AND TURN IT UPSIDE DOWN IN THE PAN , SO THATNO WATER ESCAPES FROM THE BOTTLE. MOVE THE MOUTH OF THE BOTTLE OVER THE SPACE. 7. CLAMP THE TEST TUBE, AT A 30 DEGREE ANGLE, TO SOMETHING, AND PLACE IT ABOUT 1/2 TO 1 INCH ABOVE FLAME OF THE BURNER, OR WHATEVER YOU ARE USING. DO NOT USE A GAS STOVE. AND DO NOT PLACE THE TEST TUBE OVER THE FLAME, YET. ESTIMATE, BY LIGHTING THE BURNER, AND GAUGING THE DISTANCE. 8. PLACE THE PAN CLOSE ENOUGH TO THE TEST TUBE SO THAT THE RUBBER TUBE MAY BEMOVED ANYWHERE WITHIN THE PAN. MAKE SURE, HOWEVER, THAT THE BOTTLE IS NEARERTHE FAR END. NITROUS OXIDE IS VERY FLAMMABLE. IN OTHER WORDS, JUST CLOSE ENOUGH TO THE TU
BE FOR THE RUBBER TUBING TO BE PLACED IN THE 'NOTCH OR SPACE'UNDER THE MOUTH OF THE BOTTLE. (DON'T PLACE THE TUBE THERE NOW.) 9. NOW, HEAT THE AMMONIUM NITRATE GENTLY. IF IT GETS TOO HOT, IT WILL EXPLODE, AND YOU WILL BE MISSING A FEW IMPORTANT THINGS, LIKE EYES FORINSTANCE. DO THIS BY MOVING THE BURNER IN AND OUT NEAR THE TEST TUBE KEEP THE END OF THE RUBBER TUBE AS FAR AWAY FROM THE FLAME AS POSSIBLE!!!!! THIS STEP IS TO DRIVE THE AIR OUT OF THE TUBE. AFTER ABOUT 1 MINUTE OR SO OF THIS (IT DEPENDS UPON HOW CLOSE YOU HAVE THE FALME, AND THE INTERVALS OF MOVING THE BURNER CLOSER AND FURTHER), PLACE THE END OF THE RUBBER TUBE IN THE WATER UNDER THE MOUTH OF THE BOTTLE. THE NITROUS OXIDE WILL BUBBLE INTO THE BOTTLE. WHEN BUBBLES BEGIN APPEARING IN THE WATER AROUND THE BOTTLE, SWITCH BOTTLES. AS WITH ALL HOMEMADE CHEMICALS, DO NOT STORE FOR LONG. IF YOU MUST, STORE ITIN A COOL DRY PLACE, MOUTH UP, SEALED WITH TAPE, THEN WAX. DO NOT PREPARE THE WAX NEAR THE NITROUS OXIDE. NOTES: ------ 1. YOU WILL WAN
T TO WEAR A FILTER OR A GAS MASK IF POSSIBLE, AND DO THIS INA WELL VENTILATED AREA. 2. 10 GRAMS OF AMMONIUM NITRATE, IF COMPLETELY USED, WILL FORM 5+1/2 GRAMS OFNITROUS OXIDE. THIS GAS WOULD OCCUPY 2.8 LITERS OF SPACE AT 0 DEGRESS C AND160 MM OF MERCURY, BAROMETRIC PRESSURE. SINCE TEMPERATURE WILL BE APPX. 27 DEGREES, YOU WILL PRODUCE FAR MORE THAN 2.8 LITERS. YOU WILL OBVIOUSLY NEEDMORE THAN ONE BOTTLE. HOW MUCH YOU MAKE IS UP TO YOU, BUT I WOULDN'T MAKE MORETHAN TWO BOTTLES UNLESS I HAD SOME MEANS OF COMPRESSION. AND SINCE COMPRESSIONCAUSES HEAT, IT MAY IGNITE THE NITROUS OXIDE. NOT TO MENTION THAT THECOMPRESSING EQUIPMENT IS VERY EXPENSIVE. 3. THE MATERIAL LEFT INSIDE THE TEST TUBE IS A MIXTURE OF WATER AND AMMONIUMNITRATE, HYDRATED. DISCARD IT. 4. IF NO GAS IS APPEARING, DECREASE THE INTERVALS OF MOVING THE BURNER AWAYFROM THE HEAT SOURCE. IT WILL EXPLODE IF YOU ARE NOT CAREFUL, SO FOLLOW ALLDIRECTIONS CAREFULLY. IT MAY NOT EVENBE NECESSARY TO DO THE MOVING IN AND OUT OF THE BURNER, BUT BETTER S

AFE THAN SORRY, (AND IF YOU FUCK UP, YOU WILL INDEEDBE VERY SORRY) 5. THE CHEMICAL FORMULA: NH NO --> N O + 2H O   4 3   2   2 6. MAKE SURE THAT THE TEST TUBE IS NO MORE THAT 1/4 FULL. A FLASK MAY WORKJUST AS WELL, ALTHOUGH SOME MODIFICATIONS WILL HAVE TO BE MADE. 7. AMMONIUM NITRATE IS A FERTILIZER, SO CHECK A PLANT STORE, ETC. BEWARE OFTOO MANY IMPURITIES, HOWEVER, AS THIS INCREASE THE SENSITIVITY OF THE A.N. 8. ONE LAST NOTE: 80 GRAMS WILL PRODUCE 1 MOLE OF N2O(44 GRAMS, 22.4 LITERS,AT STANDARD CONDITIONS)DISCLAIMER: THIS IS RATHER DANGEROUS. IT IS MUCH LIKE PRODUCING OXYGEN FROM POTASSIUM CHLORATE. IF YOU'VE DONE THIS (OXYGEN..) IT SHOULD BE NO PROBLEM FOR YOU. IF NOT, BE EXTREMELY CAREFUL.I AM NOT RESPONSIBLE FOR USES, ABUSES OR INJURIES AS A RESULT OF THIS FILE.

Coin Changer Fraud

Have you ever seen one of those really big changer machines in airports,
laundrymats or arcades that dispense change when you put in your 1 or 5 dollar
bill? Well then, here is an article for you.

1) Find the type of change machine that you slide in your bill length wise,
not the type where you put the bill in a tray and then slide they tray in!!!

2) After finding the right machine, get a $1 or $5 bill. Start crumpling up
into a ball. Then smooth out the bill, now it should have a very wrinkly surf
ace.

3) Now the hard part. You must tear a notch in the bill on the left side ab
out 1/2 inch below the little 1 dollar symbol (See Figure).

4) If you have done all of this right then take the bill and go out the mach
ine. Put the bill in the machine and wait. What should happen is: when you
put your bill in the machine it thinks everything is fine. When it gets to
the part of the bill with the notch cut out, the machine will reject the bill

and (if you have done it right) give you the change at the same time!!! So, yo

u end up getting your bill back, plus the change!! It might take a little pra

ctice, but once you get the hang of it, you can get a lot of money!

```
         !--------------------------------!
         !                                !
         ! (1)        /-------\      (1)  !
         !            !       !           !
         !            !  Pic. !           !
         ! (1)  /\    \-------/      (1)  !
         !      !!                        !
         !-----/  \-----------------------!

                \-------Make notch here. About 1/2 " down from (1)
```

P.S. Sorry for the "text work" but you should be able to get a good idea.

If not, I can be reached on Infinity's Edge bbs. Have fun!

<-> Hackers in the MOB <->

****

According to Schmidt, the dollar amounts are only part of the story, GTE Telemail, an electronic mail system, was broken into by at least four gangs of hackers, he says.   "They were raising hell. The system got shut down one time for a day. None of these people have been charged, nor have any of the 414s been charged yet.

"We have a major problem with hackers, phreaks and thieves," says Schmidt, who estimates that 75% of criminal hackers are teenagers and the other 25% are adults using teenagers to do their dirty work for them.

"Adults are masterminding some of this activity. There are industrial spies, people playing the stock market with the information- just about any theft or fraud you can do with a computer. There are no foreign agents or organized crime yet, but it's inevitable," he says. "I believe there are some people out there now with possible organized-crime connections.

"It's an epidemic. In practically every upper-middle class high school this is going on. I know of a high-school computer class in a school in the north Dallas suburbs where the kids are trying everything they can think of to get into the CIA computers."

"It's a strange culture," says SRI's Parker, "a rite of passage among technology-oriented youth. The inner circle of hackers say they do it primarily for educational purposes and for curiosity. They want to find out what all those computers are being used for. There's a meritocracy in the culture, each one trying to out do the other. The one who provides the most phone numbers and passwords to computer systems rises to the top of the hackers.

"For the most part it's malicious mischief," Parker says. "They rationalize that they're not really breaking any laws, just 'visiting' computers. But that's hard to believe when they also say they've got to do their hacking before they turn 18 so they don't come under adult jurisdiction. After 18, they have to do it vicariously through surrogates. They are some grand old men of hacking who egg on the younger ones... There have been some cases of a Fagin complex- a gang of kids led by one or more adults- in Los Angeles."

Who are the hackers and what secret knowledge do they have?

A 17-year-old youth in Beverly Hills, California, announced himself to other hackers on a bulletin board in this way: "Interests include exotic weapons, chemicals, nerve gases, proprietary information from Pacific Telephone..."

Prized secret knowledge includes the two area codes in North America that have not yet installed electronic switching system central-office equipment. Using this information you can call those areas and use a blue box to blow the central office equipment, and then call anywhere in the world without charge. Other secret information lets you avoid being traced when you do this.

A knowledge of the phone systems lets hackers share one of the technological privileges usually available only to large corporate customers: long-distance conference calls connecting up to 59 hackers. Schmidt estimates there are three or four conference calls made every night. The hackers swap more inside information during the phone calls.

Thanks to packet-switching networks and the fact that they don't have to pay long-distance charfus, time and distance mean almost nothing to hackers. Desktop microcompters hook into phone lines via modems make it easy to obtain copyrighted software without human intervention.

"Software piracy exists only because they can do it over the phone long distance without paying for it," Schmidt says. "some stuff gets sent through the mail, but very little. There are bulletin boards that exist solely for the purpose of pirating software. A program called ASCII Express Professional (AE Pro) for the Apple was designed specifically for modem-to-modem transfers. You can make a copy of anything on that computer. It can be copyrighted stuff- WordStar, anything. There are probably about three dozen boards like that. Some boards exchange information on breaking onto mainframes.

"In 1982 the FBI really didn't know what to do with all this information," Schmidt says. "There isn't a national computer-crime statue. And unless there's $20,000 involved, federal prosecutors won't touch it."

Since then, the public and federal prosecutors' interest has picked up. The film War Games and the arrest of 414 group in Milwaukee "created a lot of interest on Congress and with other people," FBI instructor Lewis says. "But, for ourselves it didn't really have any impact."

"We'd been providing the training already," says Jim Barko, FBI unit chief of the EFCTU (economic and financial crimes training unit). He says public interest may make it easier to fight computer crime. "There are more people interested in this particular area now as a problem. War Games identified the problem. But I think it was just circumstantial that the movie came out when it did."

Despite the help of knowledgeable informants like Schmidt, tracking down hackers can be frustrating business for the FBI. SRI's Parker explains some of the pitfalls of going after hackers: "Some FBI agents are very discouraged about doing something about the hacking thing. The cost of investigation relative to the seriousness of each case is just too high," he says. "Also, federal regulations from the Department of Justice make it almost impossible for the FBI to deal with a juvenile."

An FBI agent cannot question a juvenile without his parents or a guardian being present. The FBI approach has been mostly to support lhe local police because local police are the only ones who can deal with juveniles. Another difficulty the agency faces is the regulations about its jurisdiction.

"There has to be an attack on a government agency, a government contractor or a government-insured institution for the

FBI to have clear-cut jurisdiction," Parker says.

The FBI gets called into a case only after a crime has been detected by the complaining party. The FBI has done a generally competent job of investigating those crimes it was called in to investigate, in Parker's view. But the federal agency's job is not to help government or financial institutions attempt to prevent crimes, nor is its function to detect the crimes in the first place.

"We're not out detecting any type of crime," says Lewis. "We like to think we can prevent them. We can make recommendations. But do we detect bank robberies or are they reported to us? Or kidnapping- do we detect those? Or skyjacking? There must be some evidence of crime, a crime over which the FBI has jurisdiction. Then we open a case." And despite the spate of arrests and crackdowns last summer, it looks like the FBI will have its hands full in the future: The hackers have not gone away. Like mice running through the utility passages of a large office building, they create damage and inconvenience, but are tolerated as long as their nuisance remains bearable.

That status could change at any time, however.

Meanwhile, little electronic "sting" operations similar to Abscam keep the element of danger on the hacker's game. An Air Force telephone network called AUTOVON (a private telephone system connecting computers on every Air Force installation in the world), was reportedly cracked by a hacker last last year. The hacker published lists of AUTOVON dialups on a bulletin board.

The breach came to the attention `oo the Department of Defense on late 1983, but apparently nothing was done to stop the hackers. Then, in January, the AUTOVON number was answered in a sultry female voice. We wish to thank one and all for allowing us to make a record of all calls for the past few months. You will be hearing from us real soon. Have a happy New Year."

That's a New Year's message calculated to give any hacker a chill.

[- The Modern Speeders Guide to Radar and State Troopers -]

Introduction:

Touched off by the discussion on Ripco <312>-528-5020, I found many users asking questions about police radar, radar detectors, and speeding. With Ron Majors talking about the oil spill that will appear in detail on the news at ten I thought a informative file on the subject might be beneficial. I myself had my first experience with police radar in my fathers car, then following in baseball and my own driving, much more on the subject. What a fascinating device, that it will return your speed instantly, what fun one would be to have! After a quick talk with a police friend of mine, I soon took possession of a used police radar gun.

Part one: Operation.

Police Radar works via the doppler effect, best demonstrated by sound rather than microwaves. The doppler effect is the relation of speed to the pitch of 'sound'. Sometime, all of you must have had the distinct pleasure of being honked at by a motorist on the go, you might have noticed that the horn <an F flat on most american cars> begins with a higher pitch and as the car passes, drowns off to a lower tone. The sound waves at the front of the car are pressed together by the forward motion of the car, creating a higher pitch. As the car passes, the tone dies off to a lower pitch because the waves are spread out. Police radar works in much the same way. The major differences are the frequency and the concentration of the carrier.

As of 1988, the F.C.C. is rumored to have lifted restrictions on police radar frequencies. Before, only two frequencies were approved for police radar use. X-band <10.525 GHz> which is most commonly used, and K-band <24.15 Ghz>. I will assume for now, due to lack of any SOLID evidence supporting the restriction lift, that those are the only two in operation. Police radar 'beams' are similar in shape to a flashlight beam. They begin with a thin width and cone outwards with distance. Most guns operating at the X-band level have a range of about 2000 ft., although high power units can exceed 2500 and 3000ft., and K-band guns fall shorter at about 1200 ft.. At 1500ft., the radar beam becomes about the width of four highway lanes, so for practical purposes radars range is around 1700 ft.. A radar signal transmitted from the 'Radar Gun's' transmitter, (called the oscillator) will bounce off a object and return to the radar receiver (or antenna). If the object is moving, the frequency of the beam will be altered as it bounces. This is most easily visualized watching water ripples. Assume now that I have just dropped a pebble in a pond, and the ripples are moving outward, assume also for purposes of simplicity that the ripples are moving at 1 foot per second, and that they are one foot apart. The ripples are therefore also one second apart. Upon bouncing off a stationary object the ripples will return weakened, but at the same interval and speed <Not really the same speed, but let's not complicate things>. Now let us assume that a toy boat is traveling in the water at .5 ft. per second, 1/2 the speed of the ripples, away from the point which I dropped the pebble. Assume the first ripple has hit the boat and is traveling back. The second ripple now traveling at 1 foot per second is only gaining on the boat by .5 feet per second <1 ft. per second - .5 ft. per second>. This means that the ripple is one foot away from the boat, as the ripples are one foot apart. The ripple will take 2 second to reach the boat, as the closure speed is .5 ft. per second and the distance is 1 foot. The ripple strikes the boat and bounces back two seconds after the first ripple. The process works inversely for an object moving towards the pebbles point of impact. As the distance between the ripples can be determined by the speed, on the other side, the speed can be determined by the distance between the ripples. Police radar works in the same way with microwaves. The microwave signal

bounces off a moving vehicle and returns altered in frequency. In this way the radar unit determines the speed of the object. Radar is only accurate when the object is moving directly at, or directly away from the gun, although some modern guns will account for this 'COSINE error', most won't. Cosine error can be defined as this: When a radar signal bounces off an object at an angle from the objects direction of travel it will return a portion of the objects speed computed by the cosine of the infraction angle. If the angle of the objects direction and the radars direction is 20 degrees the speed returned by the radar is 93.97% of the objects actual speed. cos (20) = .93969262 * objects speed = returned speed. For example: A car is traveling at 75 m.p.h.. The state trooper, in his infinite wisdom, decides to "Clock" the automobile in hopes of meeting his quota for the month. Picking up his handy radar gun, he aims, and fires an invisible beam of microwave energy. The officer however, being the rookie he is, leaves a high angle between the cars direction and his beam of 45 degrees. Cos (45) = .707106781 .707106781 * 75m.p.h. = 53.03300859 53 m.p.h. is displayed on the officers screen. Lucky motorist.
Sorry 40 column users.

```
        |
        |\
        | \
        |  \       - Cosine Error -
        |   \
        | 45 \
        | deg.\ - radar beam
        |      \
        |       \
        v        \
   Direction of   \
    cars travel    \
                    \
                     X - state trooper.
```

Part 2: Application

In 1986, over 15 million speeding tickets were issued, and experts estimate that over 25% of them were in error. Police have been using radar for speed control for many years, and as the technology has become more complex and accurate, so has the ability to get away with the slight infractions of the speed limits set by the government become more difficult. In recent years, the three most damaging advances to motorists in radar technology include: A> Instant on radar. B> K-band radar. and C> Cosine error correcting radar units.

Instant on radar.

With the increase of radar receivers, or "Detectors" on the roads, police have attempted to bypass the motorists first line of defense. The most damaging advance in the war against speeding motorists is instant on radar. The idea behind instant on radar is to make the radar detector useless to the motorist by making his warning too late to react to. Instant on radar was developed in early 1983, but never marketed until late 1984 when the michigan state troopers were equipped with the first instant on radar guns. It operates by deactivating the oscillator until triggered by the officer. When used properly and under the right traffic conditions, it is indefensible. It works like a camera, the officer operating the radar will position himself behind a blind corner or over a hill. When the approaching car crests the hill or rounds the corner, the officer will activate the oscillator, taking a "snapshot" of your car. As microwaves travel at the speed of light, any attempt at slowing down is futile, the officer behind the gun has your speed in less than a tenth of a second.

K-band Radar.

When radar detectors were first marketed by the markers of ESCORT, there was only one type of radar. X-band. In an attempt to increase the dwindling speeding ticket revenue, K-band was brought to life. K-band is a different frequency that could not be picked up by the primitive detectors of the age. However, as the frequency got out, the detectors adapted, and now any detector worth a dollar will detect both X and K bands. K band is more dangerous as most K-band guns are instant on and they have less 'Splash' and range than X-band guns. This means that a K-band signal is probably closer to you.

Cosine error correcting guns.

Cosine error was a major falling of radar in the judicial system, all readings were under question in court, the result was a gun which will correct for cosine error by determining the angle which the radar beam "impacts" with the car. Also new in correcting cosin e error were guns with 'Speed lock on' in which the highest speed reading received by the gun is locked in and displayed.

Moving radar guns.

Until new developments, all radar units had to remain stationary as radar measures only closure speed, and not actual speed. Moving radar ended this trend. Moving radar works like this. First the radar gun determines the patrol cars speed by clocking a sign or fixed object. The closing speed of the patrol car to the sign is subtracted from the now taken closing speed to the target car.

Patrols speed - 60 m.p.h.
Closing speed to car - 120 m.p.h.
120 m.p.h. - 60 m.p.h. = 60 m.p.h..

Part 3: Defense

From the dawn of speed enforcement, motorists have sought to defeat the laws, starting with detectors, continuing to jammers and topping out with the new 'CHiPs detectors' The unfortunate conditions now favor the police and law enforcement officials with the introduction of new radar technologies such as instant on radar.

Detectors:

The simple radar receiver is the first line of defense from radar. Varied in operation and features, the radar detectors of today are designed to provide high sensitivity and low rates of false alarms. Good detectors will measure signal strength and type <K or X> and have an effective range of about 3000 ft. and a probable range of well over a mile. Sensitivity tops out around 110.5 dBm/cm^2 for X band and 108 dBm/cm^2 for K band <Both set by the passport>. A detector can give you an excellent advantage over radar by alerting you it's there. Detectors become especially useful in chicago where instant on radar is not typically used.

Jammers:

Radar jammers are essentially units that transmit microwaves at a frequency dictating a certain speed. The result is regardless of your speed, the police radar unit will display the speed you set the jammer to transmit. Jammers are highly illegal and will be confiscated if discovered, expect a stiff fine.

Chip's detector.

This is a new device, which is really a scanner on the police radio band. It takes advantage of a signal transmitted by the patrol cars in some states as part of their dispatch system. The signal carries for about three miles, and the Chip's Detector will alert you if you are within that range of a highway patrol unit. It also allows scanning of police radio channels.

Last words.

Radar is a basically accurate instrument, when used properly, it can be deadly. As I have said before instant on radar is impossible to avoid when there is no other traffic around, regardless of a detector. The only thing that comes close is a Radar Jammer, which will most likely not serve you well unless it is WELL hidden. Radar jammers are dangerous with the introduction of the HAWK, a radar unit by Kustom Signals, which DETECTS radar jammers in the hold mode.

Aside from radar, VASCAR
<Visual average speed computer and recorder>
is a new danger to motorists. It is basically a stopwatch used to time your movement between two point of which the interval distance is known. Using the formula Average velocity = distance / time, the state trooper can determine your speed without setting off your detector.

Instant on radar defense.

The only real defense for instant on radar is traffic. Traffic will cause the trooper to activate his radar gun more often, cluing you into his presence. A jammer well hidden will help, but the best technique is to follow a car making good time. Any police units in the area will clock him first, and legally they have to ticket him, unless you're too close.

Remember:

Do not speed, it is a dangerous practice, and I can not be responsible for any injury, or action due to this file, it is for informational purposes only. The state troopers enforce speed limits for your safety.

Radar guns: Models.

Radar guns are manufactured by many different companies, but the primary ones are Kustom Signals, M.p.h. Industries, and Decatur.

The deadliest gun now available is the HAWK manufactured by Kustom Signals. It is the first gun capable of clocking cars moving the SAME direction as the patrol car. It has two antennas, one forward, and one back. Like I stated before, it is also the first gun capable of detecting radar jammers. These run about 2000$

Kr-11

This gun is a two piece model which uses a weak pulse signal in the moving mode to determine the patrol car's speed while not triggering detectors. This gun permits a faster clocking time for instant on moving radar, it runs about $1200

Falcon

This is a hand held gun operating on K band Small and compact it is preferred among law enforcement radars. It runs about 600$

Hr-4 Hr-8 Hr-12

400,500,750$ respectively, these are hand held radar guns made by Kustom Signals

All these units are available to you via me for less than the troopers pay for them. For prices, and statistics, call my board at (312) - 787 - 2174 or send me mail at Ripco (312) 528-5020

Prices for radar units range from 250-2000$
I personally enjoy harassing that 911
who barrels by at 95 with a detector.

This is an excerpt from the BIG BROTHER GAME on opening safes via the "sound" method. Granted, this approach will not work on many safes, but keep in mind all the ones that it will... Of course, this is presented as A MATTER OF GENERAL INFORMATION and is by no means meant to be used for any purposes other than those of utmost legality.

Some safes can be opened by sound, much as in the movies, but most that were manufactured, after the mid 60's are not susceptible to the following method:

A high gain amplifier is used. A small, direct-coupled amplifier can be purchased for about 5 dollars from the various electronic supply houses. A contact microphone (i.e. one that "hears" vibrations rather than actual sound) should be employed. BE SURE to use a matching transformer if the impedances do not match; and in a pinch, a crystal phone cartridge can be employed as a contact microphone.

Place the contact mic on the safe, near the dial. Now, turn the dial 5 times to the left to clear it. Now, turn back towards the right. On the first revolution, you should hear a distinct click as the cam and lever engage. Read the number. This will be the opening number, or the last number dialed to open the safe.

Continue turning to the right. Youi will hear an additional click during the next 4 or 5 turns. This indicates how many tumblers you are actually dealing with. Most safes will have 3, but some will have 4 or 5.

While you are determining the number of tumblers, disregard the drop-in click that occurs at the opening number on each turn.

Our turning the dial to the right 5 times also perfons another duty; it clears the mechanism. This means that the dial has picked up all the tumblers and is moving them in rotation with the dial.

After jour five turns to the right, wo move the dial about 10 points BEYOND the opening number. If the opening number is 15, wi would move to 25 and stop. Now we move back to the exact opening number.

This procedure puts the opening lever and cam in position to open the safe (although the tumblers are not lined up so it will not open) now at this point, you can rock the safe dial back and forth without actually turning it.

This rocking motion causes the lever to click against the tumblers (through the lever slot). This clicking can be heard by the manipulater in his ear phones. The whole secret here is the noise will vary depending on the number of tumblers the lever is clicking against. (Much like the difference in hitting three notes on the piano at the same time, or just hitting one.)

Should we have happened to line one of the tumbler slots under the lever, the sound will be that of the lever clicking only two tumblers (as the lever will fit into the slot of the lined up tumbler, creating no sound).

Each time we rock the dial to make the lever-tumbler combination click we (assuming that there was NO difference in the sound) move the dial back to the right where it picks up the tumblers and number to realign the lever-cam slot, and repeats the rocking motion.

When you hear a sound difference, (indicating that the tumbler slot is lined up) you turn the dial back to the right until the click indicating the cam has picked up the tumblers. Now immediately stop and read the number that is lined up when you hear this click.

This is one of the combination numbers.

Now continue to the right 2 digits past the last try and move the dial back to the opening number and repeat the procedure. Do this until you have all the combination numbers.

Now, we know the opening number is the final number, but we don't know what order the combination numbers are arranged, so you will have to try all 9 (assuming 3 combinations and one opening number) possible variations. One will open the safe.

Some times you will have to move the dial a couple of points beyond the opening number to get the cam to retract the bolt and open the lock.

Some locks open to the right, i.e. R four turns 22
L three turns 18
R two turns 46
L to opening 15

Some will be the opposite (L-R-L-R).

Most locks will open no matter which way it is turned, however, a rough guideling is:

Sargent....right
Diebold....right
Yale.......left
Mosler.....left

This sort of technique will not work on high quality modern safes as they employ nylon tumblers, sound baffles, and devices to prevent the lever from touching the tumblers until ready to open. Because of this, the good agent will have a couple of alternative methods in his repertoire.

= The Science of Opening Safes =

Safes:

Once the determined agent gains successful entry to the premises, he may find that some no good son-of-a-bitch has not only placed the necessary target in a locked and alarmed building, but has also employed a safe to help insure the virginity of the target materials.

A good agent will be prepared for such an eventuality by being armed with one or more possible opening methods, and necessary implements.

Success often depends on the degree of security offered, coupled with the age and make of the safe.

Safes come in a wide variety of sizes and applications. One can encounter wall, floor, or vault models of varying thickness and offering a wide variety of resistance to the determined agent.

Most safes have at least one combination mechanism. The combination is preferred as there are no keys to lose or have copied, and the number of possible combinations varies from over 1 million to 1 billion, thus making it a bit time consuming to open one randomly.

The dial is marked with a reference point and a series of numbers. The dial is connected to the spindle which appears as a skinny metal bar and to the tumblers (which are connected to the leg bone, leg bone connected....).

The spindle transmits the motion of the dial to the tumblers, which appear as metal wheels with a cut in one spot. The tumblers are all packed together. (Do not confuse the tumblers of a safe with the tumblers of a normal lock--they are entirely different)

When the spindle turns the tumblers, they first all turn together (as each has a small metal post which hooks the next one). As the dial is stopped at the first number, that tumbler remains it that position. Then one turns the dial to the other direction moving all but that tumbler, the next number, and so on.

When all the correct tumblers are dialed in the slots will be all lined up directly under the "fence" which falls into the slots allowing the bolt to be retracted.

Sound Opening:

Some safes can be opened by sound, much as in the movies, but most that were manufactured after the mid 60's are not susceptible to the following method:

A high gain amplifier is used. A small, direct-coupled amplifier can be purchased for about 10 dollars from the various electronic supply houses. A contact microphone (i.e. one that "hears" vibrations rather than actual sound) should be employed. BE SURE to use a matching transformer if the impedences do not match; and in a pinch, a crystal phono cartridge can be employed as a contact microphone. A stethescope can be used instead of all this, but the amplifier-microphone combo is much better.

Place the contact mic on the safe, near the dial. Now, turn the dial 5 times to the left to clear it. Now, turn back towards the right. On the first revolution, you should hear a distinct click as the cam and lever engage. Read the number. This will be the opening number, or the last number dialed to open the safe.

Continue turning to the right. You will hear an additional click during the next 4 or 5 turns. This indicates how many tumblers you are actually dealing with. Most safes will have 3, but some will have 4 or 5.

While you are determining the tumber of tumblers, disregard the drop-in click that occurs at the opening number on each turn.

Our turning the dial to the right 5 turns also performs another duty; it clears the mechanism. This means that the dial has picked up all the tumblers and is moving them in rotation with the dial.

After our 5 turns to the right, we move the dial about 10 points BEYOND the opening number. If the opening number is 15, we would move to 25 and stop. Now we move back to the exact opening number.

This procedure puts the opening lever and cam in position to open the safe (although the tumblers are not lined up so it will not open) Now at this point, you can rock the safe dial back and forth without actually turning it.

This rocking motion causes the lever to click against the tumblers (through the lever slot). This clicking can be heard by the manipulator in his ear phones. The whole secret here is the fact that the noise will vary depending on the number of tumblers the lever is clicking against. (Much like the difference in hitting 3 notes on a piano at the same time, or just hitting one.)

Should we have happened to line up one of the tumbles slots under the lever, the sound will be that of the lever only clicking only two tumblers (as the lever will fit into the slot of the lined up tumbler, creating no sound).

Each time we time we rock the dial to make the lever-tumbler combination click we (assuming there was NO difference in sound) move the dial back to the right where it picks up the tumblers and then we move it about 2 digits past the last number. Now one moves the dial back to the opening number to realign the lever-cam slot, and repeats the rocking motion.

When you hear a sound differnce, (indicating that the tumbler slot is lined up) you turn the dial back to the right until the click indicating the cam has picked up the tumblers. Now immediately stop and read the number that is lined up when you hear this click.

This is one of the combination numbers.

Now continue to the right 2 digits past the last try and move the dial back to the opening number and repeat the procedure. Do this until you have all the combination numbers.

Now, we know the opening number is the final number, but we dont know what order the combination numbers are arranged, so you will have to try all 9 (assuming 3 combinations and one opening number) possible variations. One will open the safe.

Sometimes you will have to move the dial a couple of points beyond the opening number to get the cam to retract the bolt and open the lock.

Some locks open to the right, i.e.
R four turns 22
L three turns 18
R two turns 46
L to opening 15
Some will be opposite (L-R-L-R).

Most locks will open no matter which way it is turned, however, a rough guideline is:

Sargeant-right
Diebold-right
Yale-left
Mosler-left

This sort of technique will not work on high quality modern safes as they employ nylon tumblers, sound baffles, and devices to prevent the lever from touching the tumblers until ready to open. Because of this, the good agent will have a couple of alternate methods in his repertoire.

Drilling:

A good way to tell where to drill is to place your microphone against the safe about half way between the handle and the dial. Now shake the handle violently.

This should make the tail piece hit the bolt. Keep it up until you can locate the point where the noise is loudest, i.e., where the tail piece and bolt come into actual contact. Drill here.

It makes little difference whether you drill off the tail piece or bolt; either will open the safe.

It is safer to use a large bit, say one inch, on a powerful drill. This may require more than one person pushing on the drill...

Use special hardened carbide or diamond points, and always carry 4 or 5 with you.

Some safes have hardened plates covering the vital areas to discourage those who would use the method. When you encounter such a plate, press very hard on the drill and DO NOT ease up, even for a moment, as the will cause the bit to burn up.

You may have to take your torch (you did bring a torch, didn't you?) and heat the plate quite hot, let it cool, or throw water on it, drill some more, reheat, cool, drill, etc. Most hard plates are fairly thin.

Punching:

In this case, we are not referring to what the frustrated agent often resorts to when the safe fails to open, but rather, a quick method of forced entry. The agent knocks off dial off with some heavy instrument and punches the spindle with a center punch and hammer. With a bit of luck, the safe can often be opened.

However, on many high quality safes, any puching attempt will shatter the spindle, or cause the bolt to dead-lock. Some safes have a surprise in the form of tear gas which will be released when punched or burned.

Grinding:

A high speed electric grinder with a carbide wheel may be employed to cut away the safe wall around the lock mechanism.

Burning:

One of the most popular methods over the years has been the burn job.

This is accomplished with an oxy-acetylene torch. The protecting wall in front of the dial mechanism is cut away revealing the tumblers which are manipulated to open the door.

Many modern safes are laminated steel connected to something like copper, which conducts heat away from the burning area. Also one must consider the possibility of tear gas releasing at about 130 degrees.

Paper can withstand temperatures up to about 350 degrees.....

Other:

Many people feel they must go in via the door as that is the conventional way, when, in real life, the door may be the protected part of the safe.

Often, turning a safe on its top and attacking the bottom with a sledge or heavy duty axe may yield opening results. However, this method does lack a bit in the finesse department.

Peeling is another possibilty: Here one drills a hole in the corner of the door (thereby missing the anti-drill plate) and inserts a crowbar and peels back the first layer of te door. This will usually expose the locking mechanism.

One can also drill from the rear, look into the safe, decide if it is worth opening. As an added bonus, most safes can be opened by turning the dial while watching the mechanism from the rear and visually aligning the tumblers.

Thermic Lance:

A thermic lance, or burning bar, will cut through most safes with no noise, minimum hassle, and have the added advantage of being concealable and simple to operate.

I've added in an occasional hint or two in parenthesis to help some of the more uneducated phreaks understand some of the terms and whatever.

Those help phones in ATM Machine lobbies can be very useful if you have to make an emergency phone call. They work on one of two different ways. The first (and best for us) type is the kind that you pick up the phone and press a button; which activates an autodialer that calls customer service. This one generally looks like a regular traditional style wall phone without a dial and a push button somewhere near the phone instructing you to press it to get customer service. The second type can either be a phone, or is sometimes just a handset set into a mounting on the counter which tells you to pick it up for assistance. There are variations in appearance with the two types, but the button is the giveaway.

What you can do with the first type is pick up the phone and not push the button. You should just get a dialtone like in most regular phone lines, and you can dial out to anywhere by flashing the switchhook, or if the line has touchtone service, by using a portable touchtone dialer available at RADIO SHIT (er..I mean Radio Shack. Also, if you do not know how to "flash" a switchhook, consult BIOC Agent 003's Tutorials or your local phreak or phreak oriented BBS.) for $19.95. Some of these phones are hooked up to the bank's PBX (Private Branch Exchange), in which case you'll have to dial the extension for an outside line, in most places this is usually a "9", "99" or something similar. You can sometimes find out if it's on a PBX by listening to the tones coming out of the autodialer. If it puts out more than 10 digits (tones), or puts out a couple digits and pauses before dialing the rest, then it's on a PBX. Of course some autodialers mute the touch tones so you can't hear them.

With the second type you can call customer service, and either ask some stupid question, or say "Sorry, wrong number". When the nice lady hangs up in MOST cases you will get a dialtone and then you can dial out. (A lot like when you use a diverter). However if the phone line does not have touch tone, you are outta luck; as the autodialer is activated by picking up the phone, the flashing of the switchhook will false start the autodialer. So, if you can't use your TT(touch tone) pad, your outta luck.

Getting into ATM lobbies is pretty easy. They use magnetic strip card access. An ATM card obviously works, as well as credit cards, calling cards, and anything else with a magnetic strip on the back. The bolts on the door are often exposed and can be jimmied open. Some of the locking mechanisms don't even work.

There are a few things that you have to worry about. The first is that someone might notice you staying on the phone for an extended period of time, and get suspicious (This is not a BIG risk because most people could really care less what you are doing, EXCEPT for those fucking goodie-two-shoe bitches which want to make a Citizen's Arrest so that they can get in good with your local PTA). The second is that you run the risk of being recorded when you are in the lobby. Most ATM lobbies have cameras in them. Usually the camera is located in the ATM, and only goes on when a transaction in being made, but some places have 24 hour surveillance systems. These are usually externally mounted, and quite visible. If you see a camera in the lobby, don't mess around in there. The other possibility is that the phone itself could be BUGGED by the bank. According to law they are supposed to inform you with a beep every ten seconds, but no one does that anyway (NOTE: The Gestapo [Ma Bell] is supposed to notify you in the same way if they were bugging you at your home phone, but they will usually say something like "I was checking the line to see if everything was ok, and OVERHEARD some criminal dealings". This is a common way to catch people on the phone, so be careful what you say on public telephone lines.) You could do a quick look around to see if you can find anything on the line. If you don't see anything "funny", and can trace all the wiring, then you are probably safe. All in all, your best and safest bet is to use an ATM located away from a bank, and one where you can see the wiring coming from the outside to the phone. Even then, call only people who'll forget you called right after you hang up.

Audio Surveillance

Audio is the most common surveilance method in use. Most listening devices depend on some form of electronics, and it is important to understand
the usual steps to audio electronic surveillance. It is basically a 5 step process.
1) Input- usually a microphone
2) Preamplifier- used to boost the nominal signal of a mic to usable levels
3) Processing- eliminates excess noise and unwanted sounds from the output
4) Output- headphones, recorder, transmitter, etc.
5) Post-processing (sometimes)

This phile will deal with microphones. Other files will deal with each of the other steps. Microphones are judged by frequency response,
sensitivity, signal-to-noise ratio (S/N), durability, and size.
Frequency response is the range of sound that will give usable output from the mic. Human hearing is roughly 20 Hz to 20,000 Hz, but, in surveillance
work, we only need to hear the frequencies that deal with human speech.
Sensitivity is the amount of electrical output we get for a given sound level. surveillance mics need to be very sensitive to pick up the whisper
or speech from a distant room, so we look for the most sensitive mic that performs well in the other areas.
Signal-to-noise ratio is the number of decibels (dB) louder than the mic's noise the input signal is. All mics introduce hissing, cracking electrical
noise into the output. A good compact disc player can have a S/N ratio of 90 dB, totally inaudible to humans. Records give a S/N ratio of 50-60 dB,
which gives some noise during quiet passages, but a good record on a good player will have very little audible noise except during quiet parts. 50 dB
is usually considered VERY good for surveillance gear. Condenser mics give a less-than-extraordinary 35-43 dB S/N ratio. All electrical equipment
add noise to the signal. Each stage introduces more noise, so, while the noise introduced by the mic might be almost unnoticable, when added to the
inevitable noise of the other components, it can become quite annoying.
Impedance is the opposition to alternate current. This is only important because a transformer is needed to couple a mic and amp if they have
different impedences. Mics are classified either high impedance or low impedance. High impedance mics tend to lose some of their high frequency
response in long runs of cable. Low impedance mics are usually between 50 and 600 ohms. High impedance mics are in the 5000 to 20,000 ohm range.
Some mics come with built in transformers that are switchable to make them high or low impedance, but these add bulk and noise to the mic, and a
better transformer can be built into the preamplifier. It is imperative in surveillance that we match the mic impedance with interfacing machinery,
or a loss of signal and lower S/N ratio may occur.
Durability is the mic's ability to stand up to changes in humidity and temperature, as well as it's ability to withstand shock. Dynamic and
electret mics are generally the most durable.
Size is very important in surveillance work. As a rule of thumb, a small mic is always preferable because it can go unnoticed more easily than a

large one, but sometimes a large mic can be incorporated well into the environment (A large dynamic mic can be installed in a stereo speaker system and blend perfectly with the speakers inside.

There are several types of mics, but only a few are suitable for surveillance work. The most common are crystal, condenser, dynamic, and electret.

Crystal mics are microphones that use a crystal of Rochelle salt as it's piezoelectric element. Piezoelectricity is the property of acquiring oppositeelectrical charges on opposing faces of assymetrical crystals when they are subjected to pressure. It is closely related to the ceramic mic, which uses barium titanate instead of Rochelle salt. The ceramic mic is more weather resistant and has slightly lower impedance. Condenser mics have replaced crystal mics in most applications, but their high output and high impedance and low cost still find use in some applications. they find use in surveillance mainly in contact mics (such as spike mics) where a probe is linked directly to the crystal.

Condenser mics are one of the favorites for clandestine work. They are very small, offfer wide, smooth frequency response, and are fairly inexpensive. Condenser mics have to membranes, and the change in distance (which causes a change in capacitance) between them causes the electrical output. One or both of the charged membranes is flimsy, and sound alters the distance between them. They have built a built in ampifier which changes the variable capacitance to variable voltage or current, and it also drops the impedance from millions of ohms to 500-2000 ohms. It requires a power supply, usually either an internal battery or, more commonly, the mic draws power from it's output leads (often called phantom power).
Frequency response is very good. For most surveillance work, it is too good, because it reaches down below the range of human voice. The high end extends above the normal voice levels (some sopranos can reach the high end, though.)

Dynamic mics are basically speakers designed to work in reverse-instead of changing electrical signals into sound, they change sound into electrical signals. They are durable, low impedance, and very large when compared to electret mics that are a fraction of the size of a dime. They often pick up a 60 Hz AC hum unless shielded. These perform poorly in surveillance work.

Electret mics are without a doubt the best all-around surveillance mics. They work similarly to condenser mics, but require less power because they have a permanent charge across their membranes. Condenser mics use their input voltage to create a charge across the membranes.

There are other mics which just aren't cut out for surveillance work except in most unusual circumstances. The large ribbon mics used in recording studios are too expensive and fragile for surveillance work, along with giving much to wide a frequency response. Carbon mics used to be used in telephone mouthpieces, but that is fairly unusual now. They are large and give mediocre resaponse. If you ever watched mission impossible or any old spy films, you may have seen the hero unscrew the mouthpiece of a phone and take out the mic and drop in his special transmitter. It was called the drop in transmitter, and could be inserted in any "standard" phone and transmit the conversations over short distances. Pressure zone mics are perhaps the best of the uncommon mics. They are not really a mic, but a design, because they can have an electret, condenser, dynamic, etc. element in them. Pressure zone mics have a boundry about 1/32" in front of the mic. This results in the arrival of direct and reflected sound in a way that cancels echos. It enhances intelligability, but is very large. The smallest of them will fit into a shirt pocket, andthey are very expensive and fragile. Still, there are situations where they fit the bill better than any other mic.

Audio Surveillance

Audio is the most common surveillance method in use. Most listening devices depend on some form of electronics, and it is important to understand the usual steps to audio electronic surveillance. It is basically a 5 step process.

1) Input- usually a microphone
2) Preamplifier- used to boost the nominal signal of a mic to usable levels
3) Processing- eliminates excess noise and unwanted sounds from the output
4) Output- Headphones, recorder, transmitter, etc.
5) Post-processing (sometimes)

This phile will deal with preamplification. Preamplifiers boost the signal from the input to a usable level. Most microphones and sensors, such as phototransistors in light transmission bugs, give a signal that lacks power to do anything useful. The electricity generated by the needle of a record player can't drive the speakers of your stereo system.

The main factors of preamplification are gain and noise. Gain is the increase in signal given by the preamplifier. Noise is unwanted sound that the preamp generates. A good preamp can make up for a mediocre mic or a bad signal due to the location of the target with relation to he mic, but nothing can compensate for a bad preamp. A good preamp has high gain and low noise. There is no limit to the amount of gain that can be applied, but noise and electrical breakdown limit the practical application of it. Noise increases with gain, so the limit is where noise overwhelmes the signal. Electrical breakdown occurs when gain is so high that inaudible ultrasonic feedback causd by the location of the components with relation to each other causes the preamp to shut down. Electrical breakdown also occurs when gain is so high that oscillation occurs and a squeal is sent through the mic or speaker. That can sometimes be lessened by shielding or changing the location of the mic.

Operational amplifiers (op Amps) are often used because they are inexpensive, simple to use, easier to handle, and offer higher gain and lower noise than normal-component amplifiers. Op Amps are integrated circuits (ICs) that were originally developed for use in analog computers in the 1940s. They are high performance linear amplifiers with 2 inputs, allowing for inverted and non-inverted output (negative and positive gain). The gain is determined by a resistor that feeds some of the amplified signal back to teh inverting input. The smaller the resistor, the lower the gain. An Op Amp amplifies the difference between the input and ground. This may seem complicated, but it actually makes amplifier design much simpler. Even a novice could design a simple amplifier using only the Op-amp's data sheet. It is important to keep the battery leads short, but most amps avoid that restriction by using a capacitor to keep the input from oscillating. Op Amps are the components that make miniature bugs posible.

Audio Surveillance

Audio is the most common surveillance method in use. Most listening devices depend on some form of electronics, and it is important to understand

the usual steps to audio electronic surveillance. It is basically a 5 step process.
1) Input- usually a microphone
2) Preamplifier- used to boost the nominal signal of a mic to usable levels
3) processing- eliminates excess noise and unwanted sounds from the output
4) output- headphones, recorder, transmitter, etc.
5) post-processing (sometimes)

This phile deals with signal processing [steps 3 (processing) and 5 (post processing)]. Signal processing gets rid of as much unwanted noise as possible, while retaining and boosting human speech. Ideally, processing is done as the audio leaves the preamp, but that is not always possible due to size restrictions and personel availability, so we sometimes record the audio and process it later, but call it post-processing. Processing can be divided into 3 parts; speech passband, compression, and equalization.

The first step to processing is the removal of sounds outside the speech band. This makes the rest of the processing go more smoothly because the sounds that are unwanted anyway aren't dealt with. The speech passband goes from 300-3000 Hz. By eliminating the sounds outside this range, we cut the unwanted noise considerably. Filters that eliminate the sounds above and below are very easy to build (an Op Amp and a few resistors and capacitors can be thrown together to make a passable filter), but, for surveillance, we sometimes make complex filters with high dB/octave slopes. Slope measures how quickly response drops below nominative level (3 dB below input level). Steepness is expressed in dB/octave, which occurs in multiples of 6. A 36 dB/octave filter eliminates all sound below about 150 hz, and sound above that is practically inaudible up to almost 300 Hz. A 6 dB/octave filter would dampen the sounds, but they would be audible down to around 100 db, and still noticable down to around 50dB. The high end filters work the same way, only response is lower for higher signals instead of lower ones. A 24 dB slope at each end of the passband is a fair negotiation, and, to make design simpler, we could drop it to 18 dB/octave but raise the low end to 500 Hz and drop the high end to 2000 Hz and not miss much. A filter below 18 dB/octave is almost a waste of time because the filter would barely dampen the sounds that need to be removed.

The next step is compression. It would be unessacary if the target would stand in one place and speak in a clear, medium voice. Unfortunately, if you ask someone to do this, they might get a teeny bit suspicious. We all have the tendancy to speak at various levels, from a whisper to a shout, and everyone tends to move around and change the direction that they're facing when they are speaking. In a surveillance recording, we want to hear whispers as if they had been spoken aloud, and we want to hear shouts at the level of a normal voice. That's where a compressor comes into play. It raises the level of a low sound, and lowers that of a loud one. With a compressor made from an IC compander, a -80 dB signal is boosted to -40, and a +20 signal is cut to +10. The chip I use is capable of double compression, which means that a -80 dB signal is boosted to -20 and a +20 signal is cut to +5. It is possible to use 2 compressors together to bring the range within 6.25 dB of each other, but that is really unnecessary and causes the component to be bulkier than it should be. A limiter can be used with or (shudder) instead of a compressor. A limiter suppresses signals above certain levels, so your recorder or ears won't be overloaded.

The last step of signal processing is equalization. Equalization is the process of removing sounds within the speech passband that can be as annoying as those outside it. For example, if you are listening with a laser bug, your speech passband will remove 90% of the noise, and the compressor will make all the sounds audible without battering your eardrums, but the mark has a refrigarator next to the window you are useing as a reflector that is obscuring some of the sound. So you need to get rid of the narrow band that the refrigarator is on without obscuring the voices. A parametric equalizer can do the job. This is not the same as a "graphic" equalizer that you can find on a stereo system, although that can substitute if necessary. The graphic equalizer has set center frequencies and bandwidths, usually at octave points. If the sound you want to eliminate is between 2 frequencies, you have to adjust both and sacrafice some of the speech. A parametric lets you set the center frequency and bandwidth. A good parametric should operate from about 200 Hz to 4000 Hz. Anything below or above will be filtered by the passband filters. (from 200-300Hz and 3000-4000Hz will be damped, but not eliminated) A parametric equalizer with 3 bands can run rings around a graphic equalizer in the same range with 30 bands. You can also use a parametric to boost the high frequency sibilants to make speech more clear.

Audio Surveillance

Audio is the most common surveillance method in use. Most listening devices depend on some form of electronics, and it is important to understand the usual steps to audio electronic surveillance. It is basically a 5 step process.

1) Input- usually a microphone
2) Preamplifier- used to boost the nominal signal of a mic to usable levels
3) Processing- eliminates excess noise and unwanted sounds from teh output
4) Output- headphones, recorder, transmitter, etc.
5) Post-processing (sometimes)

This is the last phile in this series. It deals with the output, and what you should do with it. We can, and usually do monitor in realtime, but most intelligence work is recorded for later review. Small tape recorders introduce a LOT of noise, and don't have very long playing times. Open reel recorders correct this, but high fidelity VHS have longer recording times and better frequency response. A T-160 tape in extended play records for more than 8 hours. In addition, if the mark is under video surveillance, that can be recorded simultaniously. Pulse Code Modulation is a true digital format with better dropout compensation than VHS, and they can input to a video recorder. Digital Audio Tape also exists, and an encoder could be used easily to make your tapes useless to anyone who confinscated them. Solid state digital recorders have applications as well. Currently, the limitations are in memory only, but, with 1 megabit chips and 4 megabit chips coming into play, long play is possible. There is a device called "Memo-me" that records 32 seconds of low resolution sound on 512K. The recording time could be doubled or quadrupled without suffering much loss, and a high-memory device could be used to record for hours. Digital tape and solid state digital recording equipment is still quite a bit out of the budget of the average hobbyist, and VHS gives sufficient quality. Someday, however, the average spook will be able to feed a bad recording with unintelligable speech through his digital processor and get crystal clear sound out of it. For now, however, open reel tape offers about the best quality for the price, though most people do own a video recorder...

This was a lot shorter than I had planned. Oh, well. Anyway, watch for more philes by,

* - Chain Lock Picking - *

disclaimer:
(This document should be used for informational purposes only (hehe).)
) Don't try it (really!). As a matter o' fact teach it to others and (
(spread this phile around just so others know not to do it (ha ha ha!).)
) If you try this on any locks and get busted I can't be blamed because (
(I told you not to do it!!! (HAHAHAEHHEHEHEHOHOHHOHAHAHAH!!!!!!!!!))

===============
==EXPLANATION==
===============

This file will describe one of many ways to pick a chain lock. A chain lock is one of those locks, usually used in hotels and homes for added security, that is connected to the wall by the door and strung across the crack between the door (the side with the knob) and the wall. On the door there is a track that the knob on the end of the chain slides in. When the door is opened (with the lock locked) it is held back by the chain leaving a minimal amount of room (3-4 in.) allowing things like an eye (to see who's there), an arm (most arms), a gun, a small pipe bomb, etc... to get through. This opening can be taken to YOUR advantage when you use the extremely simple device I intend to teach you to make.

============
==CREATION==
============

When you read this part you will smack yourself and say 'That's easy! Why didn't I think of that?'. The materials you need are as follows:

= A wire-frame coat hanger (the kind totally made of wire, not the
ones with that cardboard tube)
= Long-nose pliers (if you don't have any then hands MIGHT work)
= A chain lock to pick. (duh)

Now if you know how chain locks work you will realize that you can't just squeeze your arm through the crack and release it, you must have the door closed, or almost (about 1/4 in.) closed to slide it off the track. So with the coat hanger you will slide it off. Now unravel the wire and and make the coat hanger into a straight line with only those wiggley things on the end. Then bend the coat hanger to look sorta like the diagram:

```
   |~~~~||
 Handle  \/
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ \
Catch-->   ~)_____________________________________ /
```

And with the pliers bend the wiggley end (catch) of the line to this:

```
   (~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  __)
```

=========
==USAGE==

=========

Now the Catch is used to catch the knob on the end of the cain and then push it out of the track. So the operation is simple, you just slip your arm through the hole with the end with the catch in your hand. With your

[) PAGE BREAK FOR PRINTERS (]

=USAGE=CONT'D= pg. 2

fingers, try to hook the catch on to the ring of the chain that is connected to the knob or even hook it to the knob itself. Then, close the door and slide the device toward the hinges of the door and when it goes no farther wiggle it a bit. Then push the handle toward the door to knock the knob out of it's track. Now you simply open the door and the chain should not be there anymore.

========

==TIPS==

========

When using this you might want to try different techniques in opening the lock. You could tape it to the lock or connect a rubber band to the knob then the other end of the band to the catch for maybe a wider movement range. There are many things you might want to do to make it easier and by all means improve it if you can and even sell it if you want. Also if you want to just find a way to get in touch with me and suggest!

The Art of Lockpicking

=====================

Introduction

Well, as they say, starting off is the hardest part. This applies to many things as well as the topic we are about to discuss this evening, or whenever the hell you are reading this. When I first got interested in lockpicking, it was difficult for me to find any sort of phile that explained ANYTHING at all about it. I saw a few here and there and decided that if I could compile a large phile made of many smaller philes and several peoples assorted research, (including my own) I could get one hell of an interesting little do-dad for all those aspiring little thieves out there. So here it is! But, enough of this Bull-shit.....let's get to it.....

A NOTE TO ALL FEDS, PIGS, AND OTHER ANIMALISTIC BEINGS:

```
-=>------------------------------------------------------------------<=-
-=>        !!!!!PLACE STUPID AND RETARDED DISCLAIMER HERE!!!!!        <=-
-=>                                                              <=-
-=>  This phile is intended for (as usual) information purposes ONLY!!! <=-
-=>  So if any info in this phile is used for illegal activity, it      <=-
-=>  ain't my fault or anyone else's except the particular individual.  <=-
-=>  After all, we didn't FORCE him to read this or pick any locks.     <=-
-=>                                                              <=-
-=>------------------------------------------------------------------<=-
```

Basic Picking

In the following, you will see the instruments used for picking in TEXT
form about as good as they can get.

Some things you will need to know just to start picking:

1) MANUAL DEXTERITY - If you have no self control, then don't even
think of picking locks.

2) KNOW HOW LOCK WORKS - This is very easy. It works sorta like an
engine, with the tumblers acting like the
pistons. (They move up and down)

3) CORRECT TOOLS - You can either make them or buy them. Buying is
much better. (A place to purchase lockpicks from
through mail order is listed at the end of this
article.)

4) !!PRACTICE!! - You will never be any good at lockpicking if you
don't. It is possible to pick a 5 tumbler (easy-medium lock) in under 1
minute, but that ain't gonna happen if ya don't practice. Not to mention,
if ya don't practice, and fuck up when your trying to break into something,
that extra time you take due to inexperiance could cost ya some freedom on
this great planet of ours. Get the point??????

The Entry Lock

An entry lock is a front door lock, or some sort of lock that protects
what's on the other side. These are usually 5 tumbler locks, and can be
picked with some sort of ease. Go to your local K-Mart and get an El-Chepo
entry lock and give yourself a blue dot special discount. (Either 5-finger
or price reduction.) (THIS MEANS STEAL IT DUMMY!!) Once you have this, then
take the fucker apart. This may/is easier said then done. All you will need
when you are down is the part that the key goes into. After getting that
and looking it over, you will find a cap type thing on the top of the lock.

VERY CAREFULLY TAKE THAT OFF!!! If you slip and open it too fast, the springs will go flying into a void and never be found again. The figure for the lock is figure 4.

Once the cover is off, dump 4 of the spring and tumblers into a holeless baggie (Ziplock preferred). Stick the cap back on and you are ready to use the 1 tumbler lock. This is very easy to pick, that is why you are starting with it.

Pickings

Now you are ready to pick, but what? NO PICKS? Looks like you are screwed unless you get some quick. If you are going to make them, then get some blue spring steel and a grinder. The final product mustbe about .025x .125 flat. If you already have your picks, then read on!

Take your one (1) tumbler lock and the feeler pick (fig. 1), and your tension wrench (fig. 3). Hold the lock in your other habd (ie. if you are righty then hold it in your left, and vice versa) adn stick the tension wrench into the bottom part, so that it doesn't obstruct the feeler pick as it moves in and out. Now turn the tension wrench downward (or whatever way will open your lock but usually clockwise) and insert your feeler pick. You shoudn't have to stick it in far because you are only using 1 tumbler, adn can probably see it where you are looking. Now gently push up on the tumbler, and the lock should open. If this fails to happen, then let loose on the wrench and try again. If you still can't do this, then give up, YOU ARE A LOSER IN LIFE!!! If you did open your lock, then CONGRATS!!!

After you have picked your lock, then try it again and again and again so that you get the feel of how much pressure to put on the wrench and the tumbler. When you think you hve an idea of what you are doing, open up the cap (CAREFULLY!) and stick in another tumbler (both of them) adn the spring. You should now have two tumblers installed. Now try to pick this one. Should be a little harder, but no huge difference. If it doesn't happen all at once, then try again. If you still can't do it, then this time you are NOT a loser in life, just someone who WILL have no future.

Once you are done with your 2 tumbler lock, then stick in three, then 4 and then 5 tumblers. The more there are, the harder the lock will be to pick. In one day, I got up to 4 tumblers, 5 is tricky. For less tumblered locks, a raking pick is good to use (fig. 5).

The biggest thing in in lockpicking is just getting enouf practice. Once you think you have 5 tumblers, try oyu garage door lock (locked, duh!) and see if oyu can get in. Don't worry, there will be no marks on the lock itself so MOMMY or DADDY won't shit all over you for messing with the locks.

FIGS. 1-5:

1) The Feeler Pick in TEXT

```
______________________________
\                             `---------------^,
 \____________________________,----------------'
```

The end part there goes up smoothly to a rounded end of some chicks tits.

2) What The Tumblers Look Like And The Spring

In the locks, the tumblers are different sizes (the ridges in the key should have told you that) so that is would be stupid to try and show all of the different lengths. The spring in half the size of a pen spring.
(no figure)

3) The Tension Wrench

```
_____________________________:
:
:
```

The wrench should be somewhat thicker so that it doesn't bend on your ass.

4) The Basic Tumbler Lock:

```
               CAP---,
                   \:/
   ______-------------------__
  :    IoI IoI IoI IoI IoI  :
  :    IiI IiI IiI IiI IiI  :
  =========================  :
   ---------------------------
```

o = The smaller of the two tumblers.
i = The larger of the two tumblers.
= = The passage way of the key. (KeyWay)

5) The Rack Pick (very rough)

```
________________________              ,- ,- ,- ,-
\              `-----------------  `  `  ` :
 \______________________;---------------------------'
```

This pick is just a varation of the feeler pick, 'cept that it has ridges that move the tumblers up and down fast.

Combination Locks
=================

Introduction

As you know, many people use combination locks to protect their property and personal possesions. With most, there is no keyhole, barring the ones used on regular lockers in the hall way of schools. The following will try to help you "PICK" some of the most populare combination locks used today.

-=} Picking Combination Locks {=-

Ok, so ya say ya wanna learn how to pick combination locks...This text file SHOULD help you. As a matter of fact, if ya do it right, it WILL help you. First of all, let me tell you about the set-up of a lock. When the lock is locked, there is a curved piece of metal wedged inside the little notch on the horseshoe shaped bar that is pushed in to the lock when you lock it. To free this wedge, you must(must is a word used to much) you usually(that sounds much better) have to turn the lock to the desired combination and the pressure on the wedge is released therefore letting the lock open. I will now tell you how to make a pick so you can open a lock without having to waste all that time turning the combination (this also helps when ya don't know the combination to begin with).

First of all, ya need to find a hairpin. What's a hairpin? Well, just ask your mom. She will have one. If she asks what its for, say ya gotta hold something together... If she says use a rubberband or use a paperclip, tell her to fuck off and die and then go to the store and rip off a box of 50 or so. Ok, enough stalling (yea, i was stalling).

Once you have your hair pin (make sure its metal), take the ridged side and break it off right before it starts to make a U-turn onto the straight side. The curved part can now be used as a handle. Now, using a file, file down the other end until it is fairly thin. You should do this to many hairpins and file them so they are of different thicknesses so you can pick various locks. Some locks are so cheap that ya don't even have ta file! But most are not.

Ok, now you have a lock pick. Now if ya haven't figured it out, here's how ya use it. You look at a lock to see which side the lock opens from. If you can't tell, you will just have to try both sides. When ya find out what side it opens from, take the lock pick and stick the filed end into the inside of the horseshoe-shaped bar on whichever side the lock opens from. Now, put pressure on the handle of the lock pick (pushing down, into the crack) and pull the lock up and down. The lock will then open because the pick separated the wedge and the notch allowing us thieves to open it.

Don't say bullshit until you've tried it. Because I have gotten lots of beer money from doin' this to fellow students' gym lockers. Also, this technique works best on American locks. I have never picked a Master lock before because of the shape a pressure of the wedge but if anyone does it, let me know how long it took. Also, the Master lock casing is very tight so ya can't get the pick in. So, if you're locking something valuable up, use a Master, cuz at least ya know I won't be picking it and I'm sure there aren't that many that could. And when I say pick, i don't mean lighting a stick of dynamite next to the lock, picking is opening a lock without using force, making a substitute key, etc...

```
+===========================================+
+   BE A LOCKPICK,  GET INTO PADLOCKS      +
+      "HOW TO CRACK A PADLOCK"          +
+===========================================+
```

I must attribute this message/file to reading I have done from another files about this, and some methods that I have made up on my own.

This method has been only assured with "Master" padlocks. They are a very common padlock.. This might only work on those, but who knows..

First, pull the lock down, not so much as that it is impossible to turn, but just enough to be able to do the following: Turn the knob around clockwise (to the right) until you feel a small, small resistance which will last 2-3 numbers on the dial long. You might try doing this a few times to find the exact number that it does this on, and not to be mistaken with another. Now, add 5 to the number you have gotten. Guess what? You have the first number in the combonation!

There are a few mehods to get the next number. I will tell you both, one method, is very quick, but not always 100% reliable. The other is very difficult.

QUICK METHOD: This method will get the last two numbers in the combination in one step.

--First, turn right and stop on the first number you got. Then, turn left and stop on the first number again. Continue turning to the left to the next marked number. This means that the dial goes by five, and if your first number is 18, go to the 20.. Then turn to the dial to the right again, while pulling down on the lock (as hard as you pull to unlock it if you have the right combo), and keep turning to the right until you get to the 2nd number you've tried. If it doesn't unlock, go on to the next marked number on the dial. (For instance, you're first number is 18, you tried 20 past right, it doesn't work, then try 25.) Keep doing this until eventually you unlock it, or it doesn't work. The most times that you would have to do this is about 8.

HARD, BUT NEVER FAILS METHOD: As in above, turn right to your first number, and then turn left until you get your first number again. Begin pulling down on the lock again, and trying to feel for a little resistance. If it is very stiff, you probably have the second number. If it is weak, then continue turning. You should try 2 or 3 times to make sure you get the same results. After you think you've got the second number, turn back to the right, while pulling down on the lock between tries of oh, say every 3 numbers, and eventually, CLICK, it will open.

//=DISCLAIMER: I am not held responsible for the use of this information. This is for, let's say, basic knowledge... Let's say, if you ever forget your combonation, or it is very important you get into another lock.

Miscellaneous Locks
==================

DIAL LOCKS

HAVE YOU EVER BEEN IN AN OFFICE OR SOMEWHERE AND WANTED TO MAKE A FREE FONE CALL BUT SOME ASSHOLE PUT A LOCK ON THE FONE TO PREVENT OUT-GOING CALLS?

FRET NO MORE PHELLOW PHREAKS, FOR EVERY SYSTEM CAN BE BEATEN WITH A LITTLE KNOWLEDGE!

THERE ARE TWO WAYS TO BEAT THIS OBSTACLE, FIRST PICK THE LOCK, I DON'T HAVE THE TIME TO TEACH LOCKSMITHING SO WE GO TO THE SECOND METHOD WHICH TAKES ADVANTAGE OF TELEPHONE ELECTRONICS.

TO BE AS SIMPLE AS POSSIBLE, WHEN YOU PICK UP THE FONE YOU COMPLETE A CIRCUIT KNOW AS A LOCAL LOOP. WHEN YOU HANG-UP YOU BREAK THE CIRCUIT. WHEN YOU DIAL (PULSE) IT ALSO BREAKS THE CIRCUT BUT NOT LONG ENOUGH TO HANG UP! SO YOU CAN "PUSH-DIAL." TO DO THIS YOU >RAPIDLY< DEPRESS THE SWITCHHOOK.

FOR EXAMPLE, TO DIAL AN OPERATOR (AND THEN GIVE HER THE NUMBER YOU WANT CALLED) >RAPIDLY< & >EVENLY< DEPRESS THE SWITCHHOOK 10 TIMES. TO DIAL 634-1268, DEPRESS 6 X'S PAUSE, THEN 3 X'S, PAUSE, THEN 4 X'S, ETC. IT TAKES A LITTLE PRACTICE BUT YOU'LL GET THE HANG OF IT. TRY PRACTICING WITH YOUR OWN # SO YOU'LL GET A BUSY TONE WHEN RIGHT. IT'LL ALSO WORK ON TOUCH-TONE(TM) SINCE A DTMF LINE WILL ALSO ACCEPT PULSE. ALSO, NEVER DEPRESS THE SWITCHHOOK FOR MORE THAN) A SECOND OR IT'LL HANG-UP!

FINALLY, REMEMBER THAT YOU HAVE JUST AS MUCH RIGHT TO THAT FONE AS THE ASSHOLE WHO PUT THE LOCK ON IT!

NOTE: Obviously, you needed a tiny bit of phreaking knowledge, but if it doesn't work the first time, try a couple more times. If it still doesn't work, I've got some swamp land I'd like to sell ya! (DUH!)

The Safety Chain Lock

A commonly used lock is the safety chain. Y'know, the one that you slide into the little slot along the back of your door. Well I, as well as other people have come to the conclusion that this type of lock protects you and your valuables from intruders/burglers about as much as tin foil does! While the simple method of breaking through such a pitiful barrier is to take your shoulder AND SMASH INTO THE DOOR AS HARD AS YOU CAN works well, so do bolt cutters. I will try to explain to you how to get past one of these locks quietly. After all, isn't the whole idea of lockpicking to be as quiet as is humanly possible?

First, you will need about 4 tacks, some elastic bands, and some common sense.

To defeat a safety chain lock where the door is unlocked but the chain prevents you from stealing some valuables, simply take an rubber band and somehow tie or stretch one end of the band over the knob end of the safety chain. By knob end I mean the end you would take (if you were on the other side of the door) and slide into the slot on the back of the door.

Next, take the other end of the rubber band and a thumb tack and, reaching around the back or the door as far as you can, stick the thumb tack into the back of the door as hard as you can with the rubber band rapped around or somehow affixed to the tack. Then slowly close the door. The rubber band on the back will pull the chain out of the slot for you. You can then open the door, remove the tack, and steal stuff. (Fig. 1)

```
FIG-1
-----
What the setup will look like for inside:
----------------------------------------

--------------------------        -----------------------------
                    -       -
                    -       -
         ============  -       -
~~~~~~~~~~~~~~~~~~~~     -       -  {{{{
~+        =     ()~oooooooooooooooooooo {
~~~~~~~~~~~~~~~~~~~~     -       -  {{{{
         ============  -       -
                    -       -
    (DOOR)             -       -             (WALL)
                    -       -
--------------------------        -----------------------------

                      LEGEND
                      ------
    " - "    Border of wall/door
    " ~ "    Elastic Band
    " o "    Link of Safey Lock
    " + "    Tack
    " = "    Slot For Knob of Safety Chain
    " { "    Base of Chain
    " () "   Knob Part of Safety Chain

---------------------------------------------------------------------------
```

Well, so far, most of what you have been reading has been things that I have picked up in a few scattered philes and people. Now I will begin the actual tutorial. This includes descriptions of all kinds of locks, most still being used today from the locks on your screen door, to the lock on your car.

```
----------
- PART 1 -              BASIC RULES AND PRINCIPLES
----------
```

The main key in bypassing any lock, is to know how the lock works and its design. For example. Many banks use what is called a partition lock to lock a swinging door.

```
        ---------------------
        -                  -
        -          ===      -
        -  Knob --> =   =      -      Partition Lock
        -          ===      -
        -                  -
```

When an irate customer comes barging into the bank wanting attention NOW, they may go up to the lock, and begin jerking, pulling, whatever on the little brass knob expecting to open the gate. But nada happens.. This is because the know is a phoney.. It is there with only one purpose, to fool the customer. The real way to get in is to use your finger tips and push up on the false bottom. This opens the gate. So the "key" here was to know how the lock worked.. Get it?

General Rule #1 - The Universal Key to any lock is knowledge.

General Rule #2 - Don't become keyway oriented to the point of single-
----
mindedness.

This second rule deserves some explainnation. It generally translates to, take the easiest way in/through, which is not always the door lock.. For exaple, don't try picking a difficult door lock when you have a window that you can go through. Or don't begin to focus on picking the lock without atleast checking to make sure that the door is actualy LOCKED!! (Even experts have made that mistake.) Here are a few more rules...

General Rule #3 - Know the locking mechanism perfectly.

General Rule #4 - Never give up on a practice lock opening.

General Rule #5 - When all else fails, CHEAT!

General Rule #6 - Practice on the most difficult BLT and/or lock.

Again, this rules require some explaination. The first is easy. If you are trying to pick a lock that you think is a simple warded lock but is actually a two-level tumbler, you will get nowhere fast. So know the locking mechanism. (#4) If you are trying to open a practice lock, it is ok to take 5 minute break, but after that, get right back to it. If you stop now, you may never go back. (#5) This means that if you are totally stumped by a practice lock, it is perfectly ok to open the lock up and make sure it turns the way you think it does, etc. But after that, go right back to attempting to pick the lock. Lastly, it is real impressive to pop open a disk lock in under 10 seconds, but you'll never learn how to open a high security cylinder by opening disk locks. So if a lock gives ya major trouble, keep trying it until you get it..

- PART 2 - WARDED LOCKS

Well, now that we have gone through the basic principles, let's take a look at the easiest type of lock. The Warded Lock. In warded locks the key, when inserted and turned, merely engages a locking bolt mounted in the case and slides it to the locked or unlocked position. In addition, the key may also lift or disengage a bolt retaining lever or spring; or ot may act on the bolt via an intermediary lever.

```
     -----------                   ----
     -        - <-- enters keyway  -    -        Warded Key
     -        ---------------------     -
     -------------------------------     - <-- Handle of key
      ^^^^^^^^                       -    -
     Were the patterns were cut      ----
```

This type of lock offers the bare minimum in amount of security since almost any object resembling the key will open the lock. The next step up comes when a locksmith inserts teeth called wards into the keyway or the turning path of the keybit, the end of the key that is inserted into the lock. A simple example is to cut the keyway with a tooth extending halfway into the keyway to block access. The lockmaker then cuts notches in the key where the ward would block the path. Example:

```
The Keyway:                 The Keybit:


        -----------
        -        -                -------
        -        -                -------
        -      ==-                  -----
        -      ==-                  -----
        -        -                -------
        -        -                -------
        ----------
```

The keyway would ofcourse not be square. That is just for clarity sake. The pair of "=" represetns the wards. They are in obstruction of the keyway.

This is the end of the keybit, as if it were pointing at you. The space in the middle is how the keybit bypasses the wards. It simply passes over them.

These locks eventually involed many wards within the lock, resulting in large but very figurative keys. A locksmith would usually create teh lock first including all of its wards. Then take a key with a rough outline of the wards in the lock already on it. He would then put the "blade" of the key in the center of a candle flame, coating it with soot. Then the key was inserted into the lock, turned, and removed. The markes where the wards were left tiny scratches which were then filed down. Since many people can do this simple method, security was nil. Eventually the famed "Skeleton Key" was created around this time for this type of lock which was usually an "L" shaped tool designed to bypass many different types of warded locks. You may/will find these types of locks on many 1910-1940 homes, chest, and other assorted apllication where security was either not highly required or known. Another simple security messure was to have a small peg at the end of the inside of a keyhole. Thus the pipe key, with its hallow end was made. I believe that some police handcuffs used to/still do use this method. Those stupid little locks you see on luggage etc. are usually of the warded type. The only problem these little suckers pose is that since their keyways are so small, it makes it difficult to find a pick to fit into the hole. Careful though, because these locks may also be lever tumblers which are quite different but look the same from tht outside. A look at the key can usually help you tell which is which..

Many padlocks are warded as well. But they are usually bottom of the line models. If the coer can be rotated by inserting a straight tool it is a warded lock; if not, it is a disc or pin tumbler.

BLT

Begin you BLT (Bypass Lock Technique) on warded locks. When trying to pick one of these locks, you are trying to 1)avoid all wards 2) contact and swing the bolt with enough strength without breaking the pick and getting you ROYALLY pissed off. You would be best to purchase a bunch or skeleton keys from a manufacturer for these locks.. They usually come in sets of 4-6 and are your only alturnative to making you own skeleton keys with the soot method using blanks.. Remember to becareful if you decide to cut your own keys.. If you use the same key for different locks, you MIGHT end up putting too many wards into one key thus weakening the key and it could become very uneffective, especially when it breaks off in the lock.

Now, when picking a lock, you must remember also the treatment to give a lockpick/skeleton key. DO NOT EVER use the slam-bang method like you would with your house key. Insert it slowly, feeling for obstructions until it bottoms, then turn it slowly and feel for the notch cut into the locking bolt that the key blade must contact. If you hit a solid resistance, that you have most likey hit a ward, if it is more springy thenyou have probably hit a bolt retaining spring which must also be lifted. Be sure to always carry the proper tools.. Otherwise, a simple warded lock on an old door may stop you dead in your tracks.

Warded padlocks are very common and are the perfect learning and practicing tool for beginners. You should definatly buy ATLEAST one to practice with and possibly even to attempt the soot method with.. It is good to get more than one so that you can see what different brands of locks look like inside or how to pick another warded padlock once you have conquered another.

To do this BLT, it is usually required that you pull on the shackle of the padlock to make a tension. If you are having problems, you might want to try varying the amount of tension you apply when trying to pick the lock.

That just about covers warded locks and related BLT. You should begin practicing on these locks as soon as possible to help boost your ego of actually opening a lock and not to mention, a thief that gets stopped by a warded lock looks like a complete moron. 90% of this beginning lesson should be preparation, getting the right tools, and beginning to understand locks. The other 10% should be practice.

This completes this section and your education of Basic Principles and Warded Locks. Look for:

Part 3 - Disc Tumbler Locks
Part 4 - How to Mount Practice Locks
Part 5 - Lever Tumbler Locks

....in the next phile..

* Room Entry/Lock Picking Techniques

WARNING THERE IS A HEAVILY ENFORCED LAW ON BREAKING AND ENTRY. IF YOU
GET CAUGHT FOR B&E, AND YOU ARE OVER 18, YOU WILL DEFINITELY GO TO * JAIL *...
IF YOU ARE UNDER AGED...STILL DON'T DO IT, SOME TIMES THE STUFF YOU DO STAYS ON
YOUR FUTURE RECORDS.

BACKGROUND: ----------- NINJA'S WERE ABLE TO WALK THRU WALLS, ENTER AND LEAVE A
ROOM WITHOUT A TRACE. THIS WAS ONE OF THE STEALTH SKILLS, THAT THE NINJA'S
POSSESSED. THERE WERE RUMORS THAT NINJAS CAN VANISH INTO A
WALL...WELL...THAT'S A LITTLE HOAX. YES WE ARE ABLE TO ENTER AND EXIT A ROOM
WITHOUT A LARGE TRACE...IF YOU KNOW HOW JAPANESE HOUSES IN THE ANCIENT TIMES
WERE BUILT, YOU CAN LOOK AT THE SUPPORT POSTS, THEY USUALLY HAVE GRAPPLING HOOK
MARKS IF A NINJA HAD WALKED THRU THE ROOM TO KILL A PERSON OR SOMETHING. BUT
ONE HAS TO LOOK VERY, VERY CAREFULLY.

-------------- HOW TO DO ITS: -------------- WELL...I WON'T GET INTO ANY
PHILOSOPHICAL BULLSHIT OR THE ANCIENT STUFF. I'LL GIVE YOU INFO ON THE STUFF
YOU CAN PUT TO MODERN USE.

HOW TO PICK FILE CABINET LOCKS: ------------------------------- IT'S QUITE
SIMPLE TO PICK OPEN A FILE CABINET. MOST FILE CABINETS NOWADAYS HAVE A CHEAP
DISK TUMBLING SYSTEM. IF THE DISK PATTERNS MATCH THE KEY SHAPE, PRESTO! IT'S
OPEN.

LET ME BRIEFLY EXPLAIN WHAT DISK TUMBLERS ARE...

```
        I  I  I  I  I            ****           I     I  I        ** *
****** *    <-----  KEY                          ************ *
I
I  I  I  I            ****

        ^  ^  ^  ^  ^           |--|--|--|--|           EACH ONE OF THE
```

THINGS THAT THE (^) ARROWS ARE POINTING TO ARE DISKS. (SORRY FOR THE BAD ILLUSTRATIONS.)

IF THE KEY INSERTED THRU THE 5 DISKS, AND THE PATTERN OF THE DISKS MATCH, IT OPENS.

SO TO MAKE A KEY THAT WORKS WITH MOST (ALL) CABINET LOCKS...

GET A WIRE FAIRLY THICK, JUST THIS ENOUGH TO FIT THRU THE LOCKS. BEND IT IN THE FOLLOWING FASHION.

```
                          +---- THE DISTANCE    SHOULD EQUAL
----------/\/\/\-          v     FROM TOP OF     THE DISTANCE
/\                          /      THE HUMP TO     ACROSS
TWO                          ^       THE BOTTOM OF   TOPS OR       ^
^                          +------ THE HUMP        BOTTOMS  -----|--|
```

WHEN YOU MAKE YOUR KEY, JUST INSERT IT ALL THE WAY IN. JERK IT UP AND DOWN AS FAST AS YOU CAN, AS YOU TURN THE KEY TO THE LEFT OR RIGHT, DEPENDING ON HOW THE LOCK OPENS. IF YOU GET THE HANG OF IT, YOU SHOULD BE ABLE TO OPEN ANY FILE CABINET LOCK IN A MATTER OF SECONDS. I USUALLY TAKE ABOUT 3 TO 5 SECONDS WITH MY KEY.

OPENING LOCKED DOORS: --------------------- I CAN WRITE A WHOLE BOOK IN TEACHING HOW TO OPEN LOCKED DOORS. I'LL TELL YOU THE MOST BASIC WAY OF DOING IT. THIS TECHNIQUE HAS TO BE A DOOR WITH A GAP AS WIDE AS A WIDTH OF A BUTTER KNIFE.

IF YOU HAVE A BUTTER KNIFE OR A BUTTER FLY KNIFE OR EQUIVALENT, HANDY, YOU CAN OPEN THESE KINDA DOORS AS THOUGH YOU HAVE THE KEY TO THEM.

```
         DOOR GAP             | |             | |
|-|             | |<---- THE SO CALLED "BOLT" OF THE DOOR.             |
|             |-|             | |             | |             | |

     BIRD'S EYE AND ENLARGED VIEW OF THIS



            |----------  THE KNIFE              v             I
```

```
----> SLIDE THE KNIFE THIS WAY FOR THIS PICTURE          ____ I
______             |I _|             |I/ |        DOOR             |/
|             |___|          ____|   |_______              ^
|-------------- THE "BOLT"
```

IF THE ROUND PART OF THE "BOLT" FACES YOU THEN WITH THE KNIFE, PUSH ON THE BOLT
WITH THE BACK OF THE BLADE. AS YOU PUSH, SLIDE THE KNIFE TOWARDS THE SIDE OF
THE DOOR. (SEE ILLUSTATION FOR CLARITY). YOU WILL SLOWLY MOVE IT. AND PRESTO!
THE DOOR IS OPEN. THE TRICK IS TO SLIDE THE KNIFE AND PUSHING IT AT THE SAME
TIME, AND HOLD ON TO THE DOOR KNOB. IF IT OPENS INWARDS, GET READY TO PUSH IT
AS SOON AS THE KNIFE IS THRU THE "BOLT".

FOR THE OTHER CASE (THE ROUND PART OF THE "BOLT" FACING AWAY FROM YOU), YOU
JUST PULL ON THE KNIFE AND GIVE THE SAME SLIDING MOTION. BE CAREFUL NOT TO
STAB YOURSELF. THE KNIFE'S CONTACT POINT IS ALWAYS THE BACK OF THE KNIFE.

*   Room Entry/Lock Picking Techniques Part II   *

WARNING
THERE IS A HEAVILY ENFORCED LAW ON BREAKING AND ENTRY. IF YOU GET CAUGHT
FOR B&E, AND YOU ARE OVER 18, YOU WILL DEFINITELY GO TO * JAIL *... IF YOU
ARE UNDER AGED...STILL DON'T DO IT, SOME TIMES THE STUFF YOU DO STAYS
ON YOUR FUTURE RECORDS.

HOW TO DO ITS:

HOW TO PICK 5 PIN CIRCULAR TUMBLER LOCKS:

THIS IS VERY HARD...IT TAKES A LOT OF PRACTICE TO CRACK OPEN THESE KINDS OF
LOCKS. MOST BIKE LOCKS AND ARCADE COIN SLOT LOCKS HAVE THIS TYPE OF LOCK.

LET ME BRIEFLY EXPLAIN WHAT 5 PIN CIRCULAR TUMBLERS ARE...

```
        BIRD'S EYE VIEW            _________
             ___                --=_________
            / o \          |-  ===)
           /o   o\          |-  ==)
           \_o_o_/          |-  ===)________
                          |   --=_________
                          |
                          +---  THE PINS (NOT ALL FIVE CAN BE SHOWN)
```

THE KEY IS A SMALL CIRCULAR TUBE LIKE KEY WITH A LITTLE NOTCH
AT THE END OF THE KEY, WITH FIVE SMALL DITCHES IN THE TUBE.
WHEN ALL THE PINS ARE ARRANGED SO THAT THE LOCK TURNS, PRESTO!!!
SOME HAVE SEVEN PINS....

SO TO MAKE A KEY THAT WORKS WITH 5 PIN BIKE LOCKS AND ET. AL.

MAKING THE KEY IS VERY HARD...YOU HAVE TO MAKE A KEY, EVERYTIME YOU USE IT, ONCE! THIS IS A BITCH. THE PARTS AREN'T THE EASIEST TO FIND EITHER.

FIND 5 SPRING STEEL NEEDLES THICK ENOUGH FOR STRENGTH, BUT THIN ENOUGH TO FIT INTO THE SIDES OF THE LOCKS. GET A TUBE THAT FITS THE LOCK PERFECTLY. YOU CAN KEEP THE TUBE FOREVER. TAPE THE SPRING STEEL NEEDLES ONTO THE PIPE. LET THE SPRINGS STICK OUT ABOUT 5 mm OUT OF THE PIPE. BUT MAKE SURE NONE OF THE SPRINGS ARE LAYED OUT EVENLY. NOW, INSERT IT INTO THE LOCK. GIVE IT A RAPID IN AND OUT MOTION. GET A SURGICAL SPRING NEEDLE FROM YOUR BIOLOGY LABORATORY AND USE THAT TO ROTATE THE LOCK AS YOU JIGGLE IT IN AND OUT. I HAD A HELL OF A HARD TIME PICKING OPEN A KRYPTONITE LOCK. I LOST MY KEYS TO MY BIKE AND IT WAS LOCKED TO A POLE. IT TOOK ME ABOUT 20 MINUTES. I HAD SUCCESSFULLY OPENED ONLY 5 OF THESE TYPES OF LOCKS, ONE OF THEM BEING A SEVEN PIN. IT IS VERY FRUSTRATING AND HARD. BUT WORK ON IT.

OPENING CAR DOOR TYPE 1:

I CAN WRITE A WHOLE BOOK IN TEACHING HOW TO OPEN CAR DOORS. I'LL TELL YOU THE TWO BASIC WAYS OF DOING IT. THE FIRST TECHNIQUE IS THE FOLLOWING:

A CAR WITH A LIPPED DOOR LOCK:

```
      ___
     (   )    ----- DOOR LOCK
      | |
 _________| |____________
      _
```

THESE DOORS ARE SO EASY TO PICK, IT TAKES A PRO ONLY ABOUT A SECOND TO OPEN IT. JUST GET A HANGER AND TAKE IT APART TO BE A SO CALLED STRAIGHT WIRE. BEND IT LIKE THE FOLLOWING.

```
   ____________________________
              ______

              (  L  )  L = LENGTH (ABOUT 1-1/2 INCHES)
```

THE LOOP PART OF THE HOOK SHOULD BE JUST BIG ENOUGH TO GRAB THE LOCK.

JUST STICK IT IN THRU THE SIDE OF THE WINDOW. AS YOU INSERT IT, BEND IT TOWARDS THE LOCK. IF THE GAP OF BETWEEN THE DOOR AND THE WINDOW IS TOO SMALL, THEN USE THE SECOND TECHNIQUE. AS YOU APPROACH THE LOCK AND GET A

HOLD OF IT, MAKE SURE YOU HAVE A SNUG GRIP ON THE LOCK BY TUGGING ON IT ONCE AND PULL IT IN AN UPWARD MOTION, FAST. PRESTO!!! IT'S OPEN. THIS IS VERY EASY. JUST PRACTICE ON YOUR OWN CAR OR SOMETHING, IF YOU GET A CHANCE, PRACTICE IN A SAFE LOOKING PARKING LOTS, (METRO, OR PRIVATE LOTS.) AND YOU'LL GET THE HANG OF IT.

OPENING CAR DOOR TYPE 2:

THIS ISN'T THAT HARD EITHER ONCE YOU GET THE HANG OF IT.

YOU HAVE TO GET:

A METAL RULER ABOUT AN INCH IN WIDTH AND AT LEAST 2 FOOT IN LENGTH.

CUT THE METAL NOTCH IN THE FOLLOWING FASHION.

```
     |     |
     |     |
     |_    |
      \    |
       \   |
        \  |
        /  |
      __/ /
     |   /
     |   \_
     |     |
     |     |
     |_______|
```

DO IT ACCORDING TO THE HARDCOPY'S SCALE FOR THE CUTS OF NOTCHES.
IT IS AS CLOSE TO MINES AS POSSIBLE. THEN INSERT THE STICK INTO THE SIDE OF THE DOOR. FEEL FOR A PIN INSIDE THE CAR DOOR. ONCE YOU FIND THE PIN, PUSH SLIGHTLY DOWN ON IT AND THE PULL UP FAST. BINGO! IT'S OPEN.
THIS NEEDS MORE PRACTICE THAN THE OTHER METHOD BUT IT'S NOT THAT HARD.
PRACTICE MAKES PERFECTION...SO PRACTICE HARD.

- PART 3 -   Disc Tumbler Locks

To start off, a tumbler lock is any part of the lock that is directly moved by the key and also has an unlocking function. So, the tumbler in the lock we are about to discuss is a lot like a disk, with a small rectangular looking slot cut into....about the center.

```
             _____
           _|    |_____
          |        ____| <--- Spring Finger
          |    _   |
          |   | |  |
          |   | |<------------ Key Slot
```

```
      |   || |
      |   |_|  |                    (This is BASICALLY what one
      |        |                     looks like.  Only the edges
      |_      _|                       and corners are slightly more
        |____|                           rounded.)
```

Figure 1: An individual disc tumbler

The trick is that the position of the slot can be varied, depending where the maker wants to put the key slot. It can be up slightly, further down slightly, (there are set increments, but there is no REAL reason to discuss them) but the dimentions of the slot itself never change. Now imagine that you take 5 of these disks (approx. nickel sized) and thread them onto a typical disc-tumbler key. (The key looks like your normal, average house key, only smaller. Keys to outer screen doors arean example.) Make sure that the disk you are imagining, are resting in the absolute bottom of the "V" cut on your key. (You can do this, if you like, with 5 pieces of cardboard to help you understand the concept.)

```
 __________
|        |__
|           | |  | /\|/\ | |
|    ()      \ | /\|/  |  \|/\|/\
|             \|/  |   |   |  |  \
|            __|___|___|___|__|__/
|____________| |  |  |  |  |<------ Cardboard Disks
```

(HEY! It ain't that easy drawing a key in text so give me a break ok??)

Figure 2: Cardboard practice tumblers threaded onto key cuts.

So you can see that the disks are all the same height. This is how it should be with the varied key slots through the cardboard to adjust to the different depths of the "V" cuts.

The following is the plug shown in side view.

```
  __
 | |
 | |_________________________________
 | |  _   _   _   _   _    | |
 | | |0| | | |0| | | |0< ------------ Spring Hole
 | | || || || || ||   | |
------------------------------------ <---- Key Way
 | | || || || || ||   | |
 | | |_| |0| |_| |0| |_| < ---------- Slot
 | |______________________________|__|
 | |
 |__|
```

Figure 3: View of Disk Lock Plug.

The slots in the plug hold the tumblers in place parallel to each other but allow each tumbler to move individualy. The disks protrude outward from the slots with a constant outward pressure being exerted upon the disk by little springs under the spring finger of each tumbler.

Now look at a diagram of a disk cylinder. This is what the plug mentioned and shown above slides into.

```
      _____________
     /          \
    /     ___     \
   /     |  |     \
  /     /    \     \
  |    /      \    |
  |    \      /    |
  \     \    /     /
   \     |___|     /
    \            /
     \____________/
```

Figure 4: Cylinder front view.

Notice the 2 grooves that are 180 degrees apart. When the plug is inserted, the disks coming out of the plug are lined up with these grooves. This is what holds the plug from turning thus releasing the lock. Once a correct "key" is found that will turn the mechinism inside the plug, the disk tumblers will slide down into the plug, then allowing the plug to turn within the cylinder, thus opening your neighbor's...er....your door...

The trick is to get all the tumblers at their varied hights, lined up so that they will all go into the plug and not impeade rotation. So if you had a disk tumbler lock that was loaded with all #3 depth disks, and a key with all #3 height "V" cuts, all the disk would go into the plug and you would be able to open the lock. Unfortuanly, such simple designs are never found, otherwise a straight wire could open the lock. So the lockmakers make it so all of the disk are at different depths, making it that much harder to align all of the disks at the same time. Rememeber, even 1 protruding disk will keep the lock locked.

Something to remember is that some locks have as many as 10 disks, while 5 are the most common, 6 and 7 disk tumbler locks are not too unusual.

Another type of disc tumbler lock is one that has two independent banks of tumblers that are 180 degrees apart. They fairly normal when you see them through the keyway,but they are really different because they move independently. They do tend to look like a staircase in the keyway. The way to tell for sure is by using a feeler or straight pick. Begin to manipulate one side. If both sides then move, you know that you are dealing with the normal variety. But if only one side moves, not both, you know you are dealing with independent banks of disk tumblers.

Most if not all disk tumbler locks have what is called a plug retainer. This keeps the plug from being taken out end-wise from the cylinder. They range from cams screwed in at the far end, to snap rings, to being welded together at the factory. The most common is a disc retainer. This is simply an extra disk added to the end of the plug that does not move when the key is used. Some locks have a small hole in the lock face that can be used to defeat the disk retainer when th elock is unlocked. By using a cylinder retainer shim tool (Figure 5) you can push the disk retainer into the plug and remove the plug from the cylinder.

```
|
|
|______________________________
|                     /
|------------------------/
|
|
```

(The slant on the end is usually more steep.)

Figure 5: Cylinder Shim Tool

Since most plugs have a "shoulder" on them that prevents someone from pushing them into the cylinder, they can not be accessed that way either.

Where Are They?

Here are some common applications for disc tumbler locks.

Can be found

showcase locks
telephone dial locks
office machines
cash registers
bathroom towel dispensors
gas tank covers
switch locks
other low-security applications
sidebar locks in cars (to be covered in another section)
glove compartments

Cannot be found

padlocks
exterior/interior passage lock
other high usage applications

Basic Appearance

Most of the disk tumbler keys look like your house key (pin tumbler lock) but are a little smaller, about 1/4 or an inch shorter.

Picking

Okay, you've had alot of backround shit throw at you, now let's put it to work and try to pick some locks. I recommend maybe trying your own locks around the house if you have any. In part 4, I'll tell you all the stuff you'll need to get started on mounting some prctice locks if you choose to do so.

Once you have found a lock to try, or have mounted a practice lock in wood and put it in a vise, get a tension wrench (Figure 6). Insert the tension wrench into the lock making sure that you don't block the keyway cause the raking tool in going in next (Figure 7).

```
                                   __
                                  | |
                                  | |
                                  | |
 _________________________________| |
|   ________________________________|
|  |
|_ _|
  |
  |
  |
  |
```

Figure 6: Tension Wrench

```
|
|                         /\
|________________________/  \
|                           \
|---------------------------\
|
|
```

Figure 7: Diamond pick used for raking technique

If you have a problem finding a clear place to insert the tension wrench into, look for a shallow slot at the top or the bottom of the lock and put the wrench there. This is where the key usually bottoms so that you can't insert the key into the lock too far. It is a good place to put the wrench but remember not to apply to much tension.

```
         ___________
        |//////////|
        |////////<----- Tumbler coming down from the top.
        |----------|
        |         |
        |         |
    |          |
    |___________|
    |\\\\\\\\\\|
    |\\\\\\\\<----- Shallow slot.
    |----------|
```

Figure 8: Keyway view of disc tumblers

After you insert the tension wrench into the lock, apply a little turning pressure in the direction that the lock nomally turns in. Do this until the disk bind, or cause resistance. Now insert the rake into the lock under all of the tumblers. (Note: Some locks have no backing so be careful not to stick the pick into the space behind the tumblers.)

Now, check to see if the rake moves smoothly in and out, touching all of the tumblers. If not, the rake may be too high. Grip is also a factor. Your best bet would be to hold the pick like a pencil, and let it pivot at the point where the fingers grab it. If this is not comfortable, try holding in a way that is better for you. Tension is just as important. Remember to apply CONSTANT tension, but not too little, or too much. This you will just have to determine mostly with practice. Too much tension prevents the tumblers from moving, while to little gets you just as far.

So, to recap, sum up, whatever. Apply a light, constant turning tension with the wrench, hold the pick right, putting it under all of the tumblers. Now move the rake in and out in a scrubbing motion, being sure to contact all of the tumblers on each pass, in both directions, letting the pick pivot.

If you are having trouble with the first method, here are some things you can try. Try varing the tension, but don't let off totally. Sometimes, when you ease tension while doing a stroke, the lock pops open. Remeber, too much tension can also cause your pick to bend instead of scrub, so unless you like spending money on new picks, go easy. Also, sometimes a figure eight motion works good. To try this, keep the wrist loose, and let your fingers move the pick. One last technique you could try would be the "ripping" technique. This is when you carefully insert the pick into the lock without touching any tumblers, and then ripping it out in one very fasy stroke. If you have opened the lock, CONGRATS! Do it again..and again..and again.. If not, make sure you are trying to turn the lock in the right direction. You can also check the key profile. If the key is fairly straight, with few deep "v" cuts, it is easier to open than a lock that has a key with deep "v" cuts (Figure 9).

```
 ___________
|         |_
|           |_        _     _     _
|             |____    / \   / \   / \   _
|                 \___/  \__/  \__/  \__/ \_ <--- Harder
|   ()                                  \
|                  ______________________________/
|              _____/
|            _|
|          _|
|___________|



 ___________
|     |_
|       |_
|         |____   _   _   _   _
|  ()       \___/ \___/ \___/ \___/ \_ <--- Easier
|                          \
|           _________________________/
|          ____/
|        _|
|      _|
|___________|
```

Figure 9: Two sample key profiles

Now that you've picked a disc tumbler lock (hopefully), start to notice how common these locks are. And most if not all can be picked by the same type of raking technique. After time, you'll catch on to the tensino mystery and be able to open any disc tumbler lock. The reason they are so easy to open is because they are factory made. So, since they are off of an assembly line, they have a lot of play in them. So is it wrong for us to point out the lack of quality in today's locks by picking them? Well, maybe, but who gives a shit.

- PART 4 - Practice Locks and Some Dos and Don'ts

Now that you are a practicing thief, whoops..heheh. I meant locksmith, you will need lock to practice on. I suggest getting the following types of locks:

1. Disc Tumbler Lock
2. Rim or Mortise Pin Tumbler
3. Lever Tumbler
4. Warded Mortise
5. Warded Padlock

Try to get fairly cheap ones because cheaper usually means easier to pick. You should be able to pick most up at a local store, except maybe the warded mortise lock in which case you may want to go to some second-hand store, chances are you'll get it cheaper there anyhow.

What you basically want to do, is mount the lock into a piece of wood as you would mount it into a door. Then clamp the wood in a vise. Or you could make a sort of cabinet with all the locks in one place and mount the cabinet on you wall where you can practice. Either way is fine. Just make sure you have SOME PLACE to practice. A little hint is to put the mounted lock(s), if possible, in a place where you walk often. That way you can practice every time you walk by or atleast you won't totally forget to practice a little.

Remeber to practice alot on the pin tumblers once you know how to pick them (in next phile) because they are the most common. Also, don't forget that when you are picking to sometimes practice with a flashlight because when you are out in the "field", the owner of the house will most likely not be there holding a flashlight for you. Try holding the flashlight in your mouth or even taping it to your arm. If you want, you can also try velcro.   Two fifteen minute practice sessions a day should get you well on your way.

If you have looked in catalogs for lockpicks, I'm sure you have seen those "all in one" types. Where you get 8 picks inside a pen or something. Well, take a little advice and DO NOT buy one of these. Why? Simple. When you are lockpicking, you will often need to change the type of pick you are using. So if you need two hands to unscrew the old pick, and put on a new one, whixh hand is holding the tension wrench? None. So you lose tension and have to start all over again. Gee, isn't that fun. I would suggest buying one of those leather case tools. They may be more expensive, but they are worth it. Not to mention, the companies that make those "pen picks" seem to enjoy giving us 8 picks with 5 of them being of a type you will never use in YOUR lifetime. So stick to the kits that come in cases. These are generally better quality and easier to access cause you can just drape an open case across your knee when picking.

Let's just go over the basic things to do when attempting to gain entry. First, make sure of the simple things. Like making sure the door, as well as windows and such are ACTUALLY locked. Also make sure that the door is not jammed. Check the lock also. If the lock is old and worn and requires manipulation when using the right key, do you think that you are going to be able to PICK it open. Probably not.

Next, figure out what type of lock it is. A stamped metal plate with a keyway cut into it is usually a warded lock, or a lever tumbler lock (lever tumblers will be in the next phile.) The circulaer shaped locks, like the ones on the door to your house, are usually pin tumbler, disc tumbler, or wafer tumbler locks (Schlage). On padlocks especially, if the core rotates, this could mean a warded lock. It is a lever tumbler lock if the rotating core has a slot cut in the side of it's retainer. If the core doesn't move, it is a pin tumbler.

```
|
|
|________________________________________
|___________________________________   /
|                         | /
|                         |/
|
```

Figure 10: Broken key extractor.

Next, check the keyway for foreign objects. A little trick some burglers use is to put broken toothpicks in the key way. This slows down a homeowner who could surprise an unalert burgler.

Also, make sure that you can see the tumblers. If not, they could be jammed up inside the cylinder. Something else that you may sometimes notice is that there are very few tumblers. This is because some shity locksmith put in only a few tumblers, this making the lock easier to pick. Also, make sure you know what type of lock it is. It may not be what you think.

Also, check for a brand name if visable. Certain brands like, CORBIN or RUSSWIN use or have installed slightly different parts making the lock a little harded to pick, sometimes (i.e. mushroom pins)

Next, insert the tension wrench into the plug and try to ratate it. The more it rotates, the more play is in the lock, meaning it's easier to pick. While you are doing this, try to figure out which way the plug turns. This is VERY important. If you apply tension in the wrong direction whiel picking a lock, you will never open it. You can tell the difference by the way the plug stops. If you feel an abrupt, solid stop, that is the WRONG way. If you feel a slow increase in friction to a stop, that is usually the way to turn it.

Cleaning the lock is also very important. Well, not VERY important, but it is good to know. A hint if the lock is in bad condidtion is if you smell some kind of lubricant. Chancea are that the lock is not in godd shape and the owner tried to get it to work better by shooting some WD-40 into it, which by the way is bad for locks cause it leaves a residue. Use lighter fluid to clean a lock. Gasoline and LPS-1 are also BAD to use cause of the residue left after evaporation. WARNING: Cleaning the lock with lighter fluid or naptha (another cleaning agent) leaves a smell. This will be left behind after you have gone for the homeowner or whomever to smell and shows that someone was fideling with the lock. Flush clean twice, using a straight tool to work the tumblers betwwen each washing. Then blow dry. You could try those gases in a can from cetain chemical supply house also to blow the lock dry. The purpose is to float away any dirt when cleaning and drying the lock.

Now that the lock is clean, if it wasn't already you are ready to pick it. Some people like lubricant in a lock, other don't. It is your choice, but if you do, a short squirt of powdered graphite is you best bet to use.

Also remeber to look under flower pots, rocks, etc for keys before attempting to open a lock. Just think where you might hide something, and look there.

Try to get into the routine of surveying the lock in the ways just described. If you get in a habit of it, you may not overlook something obvious when it happens. It will also help you in general to open locks.

Well, that's it for my second phile on lockpicking. In the next lockpicking phile, look for articles on:

Lever Tumbler locks &
Pin Tumbler Locks.

```
----------
- PART 5 -                Lever Tumbler Locks
----------
```

The next type of lock we will be covering in this series is going to be the lever lock. Even though it is not seen too often, we wouldn't want you to be dumbfounded the few times you do run into it. Technically, this was the next lock developed after the warded lock, it was in fact made to replace the warded lock, so you can assume that they are fairly alike.

Uses

A place where you WILL see this lock would be safety deposit boxes. But, since it is incredibly hard to pick when it is being used as a lock on a safety deposit box, most locksmith's use a "nose puller" to open the lock. This involves screwing a sheet metal screw into the key way of the box and pulling the door off the box. Some places where you will also find lever locks would be older office equipment, chests, cabinets, luggage locks, etc. Some early mortise locks are lever locks also.

Keyway

Lever locks have a unique look to them. They are a slot cut into the face of a metal cylinder with a matching slot on the collar or the lock cylinder.

```
               ---------
              -         -
             -           -
             -    []    []  <--- sometimes additional slots are cut
             -    []    -        in the collar
              -   [] <--- Keyway
               ----[]---
```

Figure 1: Lever Lock Keyway View

This cylinder or barrel or thimble or nose rises above the mounting surface, usually. It is unusual in the way that the face is free to rotate even when the key is not inserted. The key, once inside the cylinder, usually moves the boltwork directly, just like warded locks.

The Keys

The keys that are used to open these locks are often called flat keys. Why? Because that is exactly what they are. They are flat stamped keys with no side warding cuts whatsoever. The one cut they have, called the throat cut, is near the bow of the key. The key has varying rectangular depths near the tip that move the retainers to their varied height in the lock.

Time for Operation

As stated before, lever locks are much like disc tumbler locks. So, as in disc locks, the disc is the varying heights mechanisms while in lever locks it is the lever mechanism. Here the lever is moved to varying heights against a spring by a key, and then the bolt stump is free to be pushed through the aligned slots in the interior of levers from one cutout area to another.

In a lever lock, the key engages the bolt just as it would disks in disc lock. But in a lever lock, the key elevates the tumblers by rotation not my being shoved into a lock like a disc tumbler (figures 2 &3).

```
              __
             | |__
             |    |__
________________|      |
__________________________|
```

Figure 2: Key Blade (end of key) of a Lever Lock Key

```
 ____________________________________
|                    |
|      ___________         |<---(as you turn key, this entire lever
|___________|   +   |___________|    moves up.)
```

Figure 3: Lever in a lever lock.

Notice the shape of the key end. By the way, with this type of lock, the key end will always consist of rectangular cuts and no wedge profiles. You would insert the key into the lock on its side so that it lies flat. The small area marked with a plus (figure 3. The plus means nothing, it is only a marker.) is where the key would be inserted into. (The lever, figure 3, is inside the lock.) As you turn the key, you would lift up the lever bar just as you would be lifting up a disk.

The cylinder itself holds the key at the proper height in relationship to the levers and rotates the key on an axis. The tumblers will come in stacks of two, three, all the way up to fifteen. Each tumbler having a common pivot point and an individual spring. So when the key reaches is TDC (top dead center) it lifts each tumbler to its correct height based on the levels and depths of each key bitting as well as the levels of the gates (the area cutout on the bottom of the lever). If you have been following closely, you should be able to realize that this type of lock is much the same as a disc but uses retangular cuts and levers instead of wedge cuts and discs.

One small note to remember is that all lever locks of simple design are dead locks.

For picking a lever lock, a new type of technique is used, individually lifting each tumbler to its proper height. The tension wrenches for these locks are different from the ones used to pick disk tumbler locks, (figure 4) and have slight size differences. In lever locks that are most common use that type of tension wrench.

```
________________________________
                |
                |
                A
                |
                |____
```

Figure 4: Lever Lock Tension Wrench

The part of the wrench marked "A" is the part that changes. It's length may differ from wrench to wrench depending upon the lock it is meant to pick. The "A" dimension is the correct size if the wrench corresponds to the length of the key from cylinder cut to tip. If the "A" dimension is any longer than that, you will not get proper pick manipulation. You can usually buy a set somehow which generally will have four or five different sizes. You CAN try making your own, but I don't recommend it. If you absolutely must make your own, try bending one from .040 music wire and then grinding each side flat. As for lifters, your normal set that works disc and pin tumblers will also work for levers.

The basic idea behind lever tumbler picking is to apply unlocking tension on the bolt, which makes the stump bear against the inner edge of the locked position cutout. After you have tension, a lockpicker will use a lifter pick to raise each individual gate until it is lined up with the stump. The one to begin picking with is the gate in the back of the lock. When the gate and stump and gate align, the stump and gate will make contact, and the gate will catch on the stump. As long as tension is not released, the tumbler will be held in an unlocked position, even if the lifting pressure is removed. The feel of the two contacting should be quite noticeable, you might even hear it. You might also notice the tension wrench jump slightly when this occurs. You could feel a little lessening of resistance, which will come back right away if you over lift.

WARNING: do not over lift any tumbler, because this will mean that you will have to start over. This is a very common, and pain in the butt mistake. Some locks even have a little thing inside of them that detects over lifting, and will permanently lock the lock if triggered.

After you have lifted the first tumbler, the one furthest back, proceed to the next one, going from back to front. You may notice a slight lessening in tension here, or may not. The feel of the tumblers entering their gates will feel less and less as you go. After all the tumblers are lined up, the bolt moves, unlocking the lock.

Here is something that you should watch out for. In some locks, they make the cuts in the tumblers at extreme degrees. Meaning that in one tumbler they will cut it as deep as possible, while in the next, they will cut it as shallow as possible. This, by the way, is not possible with disk or pin tumbler locks. This is very good security because it becomes very difficult to lift one tumbler high enough without touching or causing misalignment with the other tumbler. So, one thing to expect with some lever tumbler locks is a high-low-high-low-high etc. combination on good locks.

Another thing is to always remember that over lifting is fatal. The only way to get the over-lifted tumbler back down is to release tension, which will probably cause all other tumblers to drop as well. Also, if a tumbler drops down right after you finish lifting it, go immediately back to it. And don't forget to go from back to front, since they usually bind strongest in back, getting weaker as you get closer to the front.

In a closing note for lever locks, let me just add that often you will come to what appears to be a small lever lock which is in actuality, merely a warded lock with a spring retainer that must be lifted before the bolt can be moved. Now while the amount of lifting you do to a retainer is not critical, for a lever lock it would be.

----------   ----------

This concludes the chapter on lever locks. If you are somewhat unclear, don't worry 'cause chances are low that you will see a lever lock. This section was added so that you can have a complete working knowledge of lockpicking if you are ever called upon to use it.

/-/   Phreak Dictionary   /-/

Here you will find some of the basic but necessary terms that should be

known by any phreak who wants to be respected at all.

Phreak : 1. The action of using mischevious and mostly illegal ways in order to not pay for some sort of telecommunications bill, order, transfer, or other service. It often involves usage of highly illegal boxes and machines in order to defeat the security that is set up to avoid this sort of happening. [fr'eaking]. v.

2. A person who uses the above methods of destruction and chaos in order to make a better life for all. A true phreaker will not not go against his fellows or narc on people who have ragged on him or do anything termed to be dishonorable to phreaks. [fr'eek]. n.

3. A certain code or dialup useful in the action of being a phreak. (Example: "I hacked a new metro phreak last night.")

Switching System: 1. There are 3 main switching systems currently employed in the US, and a few other systems will be mentioned as background.

A) SxS: This system was invented in 1918 and was employed in over half of the country until 1978. It is a very basic system that is a general waste of energy and hard work on the linesman. A good way to identify this is that it requires a coin in the phone booth before it will give you a dial tone, or that no call waiting, call forwarding, or any other such service is available. Stands for: Step by Step

B) XB: This switching system was first employed in 1978 in order to take care of most of the faults of SxS switching. Not only is it more efficient, but it also can support different services in various forms. XB1 is Crossbar Version 1. That is very limited and is hard to distinguish from SxS except by direct view of the wiring involved. Next up was XB4, Crossbar Version 4. With this system, some of the basic things like DTMF that were not available with SxS can be accomplished. For the final stroke of XB, XB5 was created. This is a service that can allow DTMF plus most 800 type services (which were not always available.) Stands for: Crossbar.

C) ESS: A nightmare in telecom. In vivid color, ESS is a pretty bad thing to have to stand up to. It is quite simple to identify. Dialing 911 for emergencies, and ANI [see ANI below] are the most common facets of the dread system. ESS has the capability to list in a person's caller log what number was called, how long the call took, and even the status of the conversation (modem or otherwise.) Since ESS has been employed, which has been very recently, it has gone through many kinds of revisions. The latest system to date is ESS 11a, that is employed in Washington D.C. for security reasons. ESS is truly trouble for any phreak, because it is 'smarter' than the other systems. For instance, if on your caller log they saw 50 calls to 1-800-421-9438, they would be able to do a CN/A [see Loopholes below] on your number and determine whether you are subscribed to that service or not. This makes most calls a hazard, because although 800 numbers appear to be free, they are recorded on your caller log and then right before you receive your bill it deletes the billings for them. But before that the are open to inspection, which is one reason why extended use of any code is dangerous under ESS. Some of the boxes [see Boxing below] are unable to function in ESS. It is generally a menace to the true phreak. Stands For: Electronic Switching System. Because they could appear on a filter somewhere or maybe it is just nice to know them anyways.

A) SSS: Strowger Switching System. First non-operator system available.

B) WES: Western Electronics Switching. Used about 40 years ago with some minor places out west.

Boxing: 1) The use of personally designed boxes that emit or cancel electronical impulses that allow simpler acting while phreaking. Through the use of separate boxes, you can accomplish most feats possible with or without the control of an operator.

2) Some boxes and their functions are listed below. Ones marked with '*' indicate that they are not operatable in ESS.

*Black Box: Makes it seem to the phone company that the phone was never picked up.

Blue Box : Emits a 2600hz tone that allows you to do such things as stack a trunk line, kick the operator off line, and others.

Red Box : Simulates the noise of a quarter, nickel, or dime being dropped into a payphone.

Cheese Box : Turns your home phone into a pay phone to throw off traces (a red box is usually needed in order to call out.)

*Clear Box : Gives you a dial tone on some of the old SxS payphones without putting in a coin.

Beige Box : A simpler produced linesman's handset that allows you to tap into phone lines and extract by eavesdropping, or crossing wires, etc.

Purple Box : Makes all calls made out from your house seem to be local calls.

ANI [ANI]: 1) Automatic Number Identification. A service available on ESS that allows a phone service [see Dialups below] to record the number that any certain code was dialed from along with the number that was called and print both of these on the customer bill. 950 dialups [see Dialups below] are all designed just to use ANI. Some of the services do not have the proper equipment to read the ANI impulses yet, but it is impossible to see which is which without being busted or not busted first.

Dialups [dy'l'ups]: 1) Any local or 800 extended outlet that allows instant access to any service such as MCI, Sprint, or AT&T that from there can be used by handpicking or using a program to reveal other peoples codes which can then be used moderately until they find out about it and you must switch to another code (preferrably before they find out about it.)

2) Dialups are extremely common on both senses. Some dialups reveal the company that operates them as soon as you hear the tone. Others are much harder and some you may never be able to identify. A small list of dialups:

1-800-421-9438 (5 digit codes)
1-800-547-6754 (6 digit codes)
1-800-345-0008 (6 digit codes)
1-800-734-3478 (6 digit codes)
1-800-222-2255 (5 digit codes)

3) Codes: Codes are very easily accessed procedures when you call a dialup. They will give you some sort of tone. If the tone does not end in 3 seconds, then punch in the code and immediately following the code, the number you are dialing but strike the '1' in the beginning out first. If the tone does end, then punch in the code when the tone ends. Then, it will give you another tone. Punch in the number you are dialing, or a '9'. If you punch in a '9' and the tone stops, then you messed up a little. If you punch in a tone and the tone continues, then simply dial then number you are calling without the '1'.

4) All codes are not universal. The only type that I know of that is truly universal is Metrophone. Almost every major city has a local Metro dialup (for Philadelphia, (215)351-0100/0126) and since the codes are universal, almost every phreak has used them once or twice. They do not employ ANI in any outlets that I know of, so feel free to check through your books and call 555-1212 or, as a more devious manor, subscribe yourself. Then, never use to your caller log, they can usually find out that you are subscribed. Not only that but you could set hack away, since they usually group them, and, as a bonus, you will have their local dialup.

5) 950's. They seem like a perfectly cool phreakers dream. They are free from your house, from payphones, from everywhere, and they host all of the major long

distance companies (950-1044 <MCI>, 950-1077
<Sprint>, 950-1088 <Skylines>, 950-1033 <Us
Telecom>.) Well, they aren't. They were designed for
ANI. That is the point, end of discussion.

A phreak dictionary. If you remember all of the things contained on that fileup there, you may have a better chance of doing whatever it is you do. This next section is maybe a little more interesting...

Blue Box Plans:

These are some blue box plans, but first, be warned, there have been 2600hz

use a 2600hz tone for a few very naughty functions that can really make your day

lighten up. But first, here are the plans, or the heart of the file:

700	1	2	4	7	11
900	+	3	5	8	12
1100	+	+	6	9	KP
1300	+	+	+	10	KP2
1500	+	+	+	+	ST
	700	900	1100	1300	1500

Stop! Before you diehard users start piecing those little tone tidbits together, there is a simpler method. If you have an Apple-Cat with a program like Cat's Meow IV, then you can generate the necessary tones, the 2600hz tone, the KP tone, the KP2 tone, and the ST tone through the dial section. So if you have that I will assume you can boot it up and it works, and I'll do you the favor of telling you and the other users what to do with the blue box now that you have somehow constructed it. The connection to an operator is one of the most well known and used ways of having fun with your blue box. You simply dial dial '0') and blow a 2600hz tone through the line. Watch out! Do not dial this

KP tone to start a call, a ST tone to stop it, and a 2600hz tone to hang up. Once you have connected to it, here are some fun numbers to call with it:

0-700-456-1000 Teleconference (free, because you are the operator!)
(Area code)-101 Toll Switching
(Area code)-121 Local Operator (hehe)
(Area code)-131 Information
(Area code)-141 Rate & Route
(Area code)-11511 Conference operator (when you dial 800-544-6363)

Well, those were the tone matrix controllers for the blue box and some other helpful stuff to help you to start out with. But those are only the functions with the operator. There are other k-fun things you can do with it.

More advanced Blue Box Stuff:

Oops. Small mistake up there. I forgot tone lengths. Um, you blow a tone pair out for up to 1/10 of a second with another 1/10 second for silence between

the digits. KP tones should be sent for 2/10 of a second. One way to confuse the

2600hz traps is to send pink noise over the channel (for all of you that have decent BSR equalizers, there is major pink noise in there.) Using the operator functions is the use of the 'inward' trunk line. That is working it from the inside. From the 'outward' trunk, you can do such things as make emergency 'stacking'), enable or disable the TSPS's, and for some 4a systems you can even re-route calls to anywhere.

All right. The one thing that every complete phreak guide should be without is blue box plans, since they were once a vital part of phreaking. Another thing that every complete file needs is a complete listing of all of the 800 numbers

/-/ 800 Dialup Listings /-/

1-800-345-0008 (6)
1-800-245-4890 (4)
1-800-526-5305 (8)
1-800-437-9895 (7)
1-800-343-1844 (4)
1-800-437-3478 (6)
1-800-547-6754 (6)
1-800-327-9136 (4)
1-800-858-9000 (3)
1-800-245-7508 (5)
1-800-322-1415 (6)
1-800-325-7222 (6)

All right, set Cat Hacker 1.0 on those numbers and have a fuck of a day. That is enough with 800 codes, by the time this gets around to you I dunno what state those codes will be in, but try them all out anyways and see what you get.

On some 800 services now, they have an operator who will answer and ask you for your code, and then your name. Some will switch back and forth between voice and tone verification, you can never be quite sure which you will be up against.

Armed with this knowledge you should be having a pretty good time phreaking now. But class isn't over yet, there are still a couple important rules that you should know. If you hear continual clicking on the line, then you should assume that an operator is messing with something, maybe even listening in on you. It is a good idea to call someone back when the phone starts doing that. If you were using a code, use a different code and/or service to call him back.

A good way to detect if a code has gone bad or not is to listen when the number has been dialed. If the code is bad you will probably hear the phone ringing more clearly and more quickly than if you were using a different code. If someone answers voice to it then you can immediately assume that it is an operative for whatever company you are using. The famed '311311' code for Metro is one of those. You would have to be quite stupid to actually respond, because whoever you ask for the operator will always say 'He's not in right now, can I have him call you back?' and then they will ask for your name and phone number. Some of the more sophisticated companies will actually give you a carrier on a line that is supposed to give you a carrier and then just have garbage flow across the screen like it would with a bad connection. That is a feeble effort to make you think that the code is still working and maybe get you to dial someone's voice, a good test for the carrier trick is to dial a number that will give you a carrier that you have never dialed with that code before, that will allow you to determine whether the code is good or not. For our next section, a lighter look at some of the things that a phreak should not be without. A vocabulary. A few months ago, it was a quite strange world for the modem people out there. But now, a phreaker's vocabulary is essential if you wanna make a good impression on people when you post what you know about certain subjects.

/-/ Vocabulary /-/

phone -> fone
freak -> phreak

- Never substitute 'z's for 's's. (i.e. codez -> codes)

- NEVER use the 'k' prefix (k-kool, k-rad, k-whatever)

- Do not abbreviate. (I got lotsa wares w/ docs)
- Never substitute '0' for 'o' (r0dent, l0zer).

- Forget about ye old upper case, it looks ruggyish.

All right, that was to relieve the tension of what is being drilled into your minds at the moment. Now, however, back to the teaching course. Here are somethings you should know about phones and billings for phones, etc.

LATA: Local Access Transference Area. Some people who live in large cities or areas may be plagued by this problem. For instance, let's say you live in the 215 area code under the 542 prefix (Ambler, Fort Washington). If you went to dial in a basic Metro code from that area, for instance, 351-0100, that might not be counted under unlimited local calling because it is out of your LATA. For some LATA's, you have to dial a '1' without the area code before you can dial the phone number. That could prove a hassle for us all if you didn't realize you would be billed for that sort of call. In that way, sometimes, it is

better to be safe than sorry and phreak.

The Caller Log: In ESS regions, for every household around, the phone company has something on you called a Caller Log. This shows every single number

that you dialed, and things can be arranged so it showed every number that was calling to you. That's one main disadvantage of ESS, it is mostly computerized so a number scan could be done like that quite easily. Using a dialup is an easy

way to screw that, and is something worth remembering. Anyways, with the caller log, they check up and see what you dialed. Hmm... you dialed 15 different 800 numbers that month. Soon they find that you are subscribed to none of those companies. But that is not the only thing. Most people would imagine "But wait! 800 numbers don't show up on my phone bill!". To those people, it is a nice thought, but 800 numbers are picked up on the caller log until right before they are sent off to you. So they can check right up on you before they send it away and can note the fact that you fucked up slightly and called one too many 800 lines.

Right now, after all of that, you should have a pretty good idea of how to grow up as a good phreak. Follow these guidelines, don't show off, and don't take unnecessary risks when phreaking or hacking.

Homemade Silencers

This is a phile on building a firearm noise suppresser. It can be made simply out of cardboard and glue. First, a word on "silencers." The term is a nice one, but very inaccurate. Anyone with more than a layman's knowledge of guns would call them a firearm noise suppresser, but that is also somewhat misleading. They both sound as if they are a device that either eliminates or muffles the sound of a gun being fired. It really changes the way it sounds. A "silenced" shot can also make sounds of up to 110 dB, but, if someone shot a gun near you, you wouldn't think,"That sounds like a muffled gunshot," you'd think "I wonder what that sound was?" The sound that it makes depends upon the suppresser, the weapon, the caliber, and the ammunition. Basically, there are 3 ways suppressers are made. Either with baffles (little washer-type things spaced at regular intervals along the body of the silencer), screen (wire mesh wound around the inside walls of the tube), or a combination of the two. For simplicity, this one will use baffles only, but anyone could adapt it to screen or a combination.

First, you need a tube. A roman candle casing would do the trick nicely, or any parallel wound casing of sufficient length, or you could use good, sturdy PVC piping. I wouldn't use metal, cause the tube will turn into lethal shrapnel if there is a problem. You can use metal washers, or just cardboard ones, but you should use the sturdiest type you can find. you can also use copper or steel scrubbing pads if you want to make a screen version. Optimally, the tube should friction-fit snugly around the gun barrel, but you may not have a convieniently sized tube around, so you can just wrap some duct tape around the barrel of your gun until it fits right. DO NOT TAPE THE SUPPRESSER TO THE GUN BARREL! Wrap the barrel with tape evenly until the outside diameter is wide enough to hold the suppresser on. You should use cardboard baffles for your first try, and center them as well as you can. If a bullet hits a carboard baffle, it will just keep going at a reduced speed. If it hits a metal washer, it will probably ricochet off and leave the tube through the side, if at all, so you should be extra careful when using metal parts. Now, here's how to make it.

Make some baffles out of cardboard. This is a little tricky, cause a badly placed baffle could be dangerous, and would destroy the silencer. These can be made either as circles or as circles with flaps to hold them on. The second type will make for a more durable and longer lived suppresser. Then glue them onto the tube spaced regularly, 3/8" to 1/2" should do it. The tube should be from 8" to 10" long. Leave about 1 1/2" to 2" on one end to go over the barrel. If you have a sight on the gun, you'd be better off removing it, but you can cut a channel with an exacto knife for it. The baffles should have a hole in them slightly larger than the diameter of the ammunition. Here's the diagram:

```
      -------------------------------------------
 --------------  I  I  I  I  I  I  I  I  I  I
 ==============
 --------------  I  I  I  I  I  I  I  I  I  I <---baffles
  ^    -------------------------------------------
  I                    ^
  I                    I
gun barrel                  I
```

cardboard tube or
PVC pipe

BTW, don't build this. Firearm Noise Suppressers are legal in some states, but they require a serial number and a $200 tax for each of them. Even still, it is dangerous to make something like this, and I strongly suggest you don't try it. If you absolutely HAVE to, at least use a low charge 22 pistol or, better, rifle. I suppose this design would even have an effect on a pellet or BB gun, because it suppresses the sound of the expanding gasses coming out of the barrel. I take no responsibility for what you do with this info, etc., etc. That's about it. Watch for more by,

(> Credit Cards <)

Well when they made the credit card they put three things on it, which were supposed to be top secret, they did not want a person to know what they did or what was behind them. The three things I'm talking about are: the account number, the signature panel, and the magnetic strip.

Well let's see here, most things I have seen have 6-10 digits right? Yet credit cards have around 20 digits, why? Well its not necessary of course for a credit card to have that many, but it does! Each card holder must have a unique number of course though. Visa has maybe 70 million card holders at this time, Mastercard too. Which leads us to 70 million available numbers!

There are one hundred million possible combinations of eight digits, from 00000000 to 99999999. So eight digits would be enuf. To allow for future growth, Visa could have 9 digits-enuf for one billion different numbers!

In fact, a Visa card has 13 digits and sometimes even more. And American Express has 15 digits. Diners Club cards have 14. Carte Blanche has 10. They are obviously not expecting billions of card owners with those digits. But all the extra ones are only a security device. I mean if they were 4 digits each most people would have no problem getting themselves 3232 fake credit cards!

Say your Visa number is 4321 876 132 564. Each purchase must be entered from a sales slip. The account number tags your purchase to your account. Sometimes the sales people get bored and enter the wrong number. There are 10 trillion possible 13 digit Visa numbers. Only about 65 million of those are working accounts! Which means it is very hard to find one. Those are slim odds to find the number you could fill up a book full of 13 digit numbers. Still you would not duplicate a Visa account number.

Then we have Mastercard of the quadrillion possible combos only about 11 million are active accounts. Among other things, that makes it possible for them TV, radio and other ads to invite card holders to call up and order. How can they be sure the guy even has a card?

They must base there confidence on the security of the credit carding system. If someone calls up even making sure to use the right number of digits the number will surely not exist. To be practical the only way to get a credit card number is to get it right off the plastic card.

So how do I get the credit card numbers you ask? There are two very easy ways that you can use anytime, one is getting it off the old copy that was run off in the store, so if they don't throw the copies away pick them up and it's yours..then you can also do this very simple trick over the phone:

You: This is bank 1. We are calling to tell you that the credit limit on your Mastercard has been raised to twelve hundred dollars.

Person: but my limit has always been 10,000 dollars!!!

You: Hmmm.. There must be some error or problem in the computers. Do you have your card handy? Could you read off the number?

Right there the person is very worried and wants his limit back so of course he gives you the number.

The signature panel and magnetic strip will be covered in later volumes.

(> Alarms and Fingerprints <)

Lets make this fast so we can get to the lie detector part. This trick is quite simple. You walk into a big business office that has it so you must enter a certain number of digits before you can enter. Then it will open the door for you. So you go over and clean off the panel and wipe out all the fingerprints, stand outside the door and wait for a guy to go in. He will punch the numbers and go in. Take out sum fingerprint dust and you will see the digits. Write them down....you now know that those digits in some kind of order open the door!

> The Void Pop Up <

What happens if you Xerox something you're not supposed to? Like money, stock certificate, or coupons... Well the copy usually comes out all yucky huh? But...if you use a good color copier you can usually produce a good, convincing counterfeit.

The void pop up is what tries to stop all this from being done. It's a secret gimmick made to waste all us counterfeiters. When the document is copied that contains this gimmick a big 'VOID' will pop up. The void is hard to see, but the people who use it think that it must take a lot more guts to pass around it even with a hard to see void then without it.

The American Bank Note Company invented this void pop up deal, but they didn't patent it. So everyone decided to use it themselves. It's become a common security device for most mediums...like Kentucky Fried Chicken, banks and other things.

The void pop up uses a screen - some dots that only appear as a grey pastel shade. The only thing that shows a difference is how dark the grey is. But it depends, the bigger the area the 'void' pop up covers the darker the grey.

Two screens could look different from the human eye, only because they grey was put on top of another color or by another color.

One of the screen prints the 'void' and the other makes the background for the letters to show up on.

See, a Xerox machine sees differently then a human eye does. One of the screens is chosen so the configuration. Dots will bleed together when copied. The screen comes out darker and in differ quality, leaving the 'VOID' visible.

But wait, the system is not foolproof, because copiers vary. So the void is shown clearly on some machines and hardly noticeable on others.

Occasionally you can see a faint void on the original. So the poor people who don't even know about it can get in trouble for not even doing anything. There are some screen attachments for some copiers which will defeat the void pop up system, they will make a clean copy. This is bad for the people that use the void pop up technique, because in the future the copiers will just get better and better which means they will probably have to come up with a new idea to defeat them. Ha! There are other ways too so they are not in trouble they can still find ways to stop illicit photo copying. The 'prospects/new book news' is a New York newsletter, it is printed on red paper. Red shows up nearly black on black-and-white photo copiers so it would be quite hard to read huh? But 'prospects' could be copied on a color copier, and the black-n-white machines that have red filters.

A light blue will not show up on copiers though so in a lot of publications they will now use a type of light blue pen to write in.

Here is what computer world said about the light blue print:

The Diners Club, whose accounting system has been attacked by people trying to keep their accounts straight has found away to keep the complaint level down -- especially the kind that are copied to various federal and state authorities.
It won't stop the complaints entirely but will reduce the effectiveness in many cases.

What the Diners Club did was redesign the forms, printing much of the data in a non-reproducing blue. As a result, after it was stuck in the copy machine the output is unreadable, and certainly not very easy to read by the people who want to!

But according to he Diners Club the light blue was just a coincidence, the logo was blue.

=> Free Keys <=

The subject of the matter is keys, keys that can get us into: pop machines, stamp machines and many more things.. The locks are quite hard to pick because of the way they are made inside the little circle, so we have come up with he ultimate duplicating idea.

That is to take an air drying substance like a clay mix, pottery mix a kind of matter like that. When you have it stick it in until an impression is made, take it out and when it has dried you have yourself a working key.

Now if you are a locksmith or know a locksmith then you can give that to him and maybe he can transfer or you can transfer it into a real stainless steel key!

I suggest using this in hotel machines and other machines that people are not around all the time so you don't get caught, always make a backup of the key in case on gets smooshed.

=> The Eye Test <=

A test everyone wants to cheat on, it's the most boring and stupidest for people that already have good vision...if not I suggest not cheating on it! To qualify for 20/20 vision you must be able to read line 8 perfectly...you can mess up all the others just know line 8. No one is supposed to know this because if they did all they would have to do is find line 8, right? Exactly...there are only 9 letters used on the eye chart so common letters that you might think like is a 'G' is really a 'C' or an 'O'. Here is the eye test:

LINE 1: E

LINE 2: F P

LINE 3: T O Z

LINE 4: L P E D

LINE 5: P E C F E D

LINE 6: E D F C Z P

LINE 7: F E L O P Z D

LINE 8: D E F P O T E C

LINE 9: L E F O D P C T

LINE 10: F D P LT C E O

LINE 11: P E Z O L C F T D

Good cheating!

=> Crest Toothpaste - Deadly & Sick? <=

Hey man there is really secret ingredients in Crest huh? So the rumors say....so what they be?

Sand & rat poising..

Oh interesting ill stick with Crest..

Well yes its true that Crest contains these matters but not like they seem, yes I guess you could say there is sand 'hydrated silica' it says on the crest label.. Which is a type of sand, if you are willing to trace it back far enough down the raw materials cycle you will end up with sand.

You! Crest has fluoride which really prevents cavities, you know what it is? Well fluoride is sodium fluoride.. sodium fluoride in turn is a chemical used in rat poising which will kill rats and is toxic to humans...once in a hospital it was mistaken for dry milk and some people died...but of course the level of it contained in Crest is *far* below the toxic level so there is no need to worry..

=> Secret Things <=

Here it is all those secret things that we really should not know...here are a few for this volume:

Ma Masion is a secret restaurant in Los Angles, they keep all the low lifes out with an unlisted number: (213) 655-1991

Well you know Samsonite luggage? Well there is a South African kind now called: Saxony, it looks exactly like Samsonite but has a secret false bottom to be used for smuggling..

The Bank of America in Beverly Hills, CA, Branch 9461 Willshire Blvd has a nice quiet upstairs for it's wealthy depositors, with no waiting in line for tellers...

Introduction

Videocrypt is a pay-tv scrambling system jointly developed by Thomson Consumer Electronics and News Datacom.   Over one million users receive Videocrypt encrypted signals and this system, has to date, remained secure from illicit decoder manufacturers, protecting the revenue of Videocrypted television channels.

Requirements

Videocrypt is a multi-standard encryption system which is suitable for PAL, NTSC and SECAM transmissions. Language is no barrier for Videocrypt with its capacity for multi-lingual transmissions and broadcasts utilising a comprehensive on-screen instruction menu.

Features and applications

A smart card is the central key to the Videocrypt system, and the card can be used for a variety of diverse applications. The card is pre-coded to determine a users requirements and it can subsequently be addressed utilising the decoders logic to amend the users services at the broadcasters will.

There are a number of broadcasting modes which the smart card can be used within including:

Clear Mode
Signals sent in the clear are recognised by the decoder and passed to the display without further processing.

Free Access
Pictures transmitted with an encryption key are delivered directly to the display through the decoder.

Controlled Access
Access to encrypted pictures is determined by the level of access authorised to the users smart card. No signals will be transmitted in an unencrypted state without prior authorisation.

Programmes can be tailored to usage with the Videocrypt system and the system offers a flexible way for pay-tv operators. There are a number of operations mode offered as standard including:

* Single or multiple subscriptions with many tier levels in one channel

* Pay Per View (PPV) and impulse purchasing

* Thematic selection (enable all arts programming)

* Geographic limitation (restrict to a country/area)

* Single-event (throwaway cards)

* Parental Control (reception with card only)

* Pre-determined time period

Videocrypt enables smart cards to be pre-programmed to suit the specific programming requirements.

Smart card - providing the revenue security

Security can be addressed on a multitude of levels when using the smart card. These include:

Chaining

An existing customer would receive a new card which contains part of the new code, the remainder of the code would be transmitted when the card is inserted into the decoder and the subscriber compiles with the instructions contained within the on-screen graphics.

Over-the-air addressing

Systems operators can now address individual subscribers, which is a vast improvement over other scrambling systems. The operator can provide additional services, reduce service entitlements, send individual messages, blacklist and/or whitelist viewers.

Cloning

A number of steps have been taken to stop smart cards being copied or cloned. A physical deterrent is the first line of defence, and the integrated circuit contained within the card makes "probing" very difficult as the IC is likely to become damaged in the process.

Cost is a second factor which is likely to deter manufacturers of illegal decoders. A considerable amount of time, trouble and expensive resources would be required to clone the card.

The manufacturers of Videocrypt recommend that the cards are replaced every six months, and each time this is done a "secret encrypting algorithm" will be changed. Any pirate decoders manufactured during this time would be relatively useless.

And should a pirate decoder be manufactured, it will contain a unique security code, which could be blacklisted by the systems operator once the code has been discovered - leading to calls of complaint by angry customers.

Video taping

Videocrypt offers an simple method of tracking down pirates who video high-value programming and then distribute it.

The customers unique number can be displayed on the unencoded screen for reference and future litigation. Although an on-the-screen code can be generated for signals piracy in a public place, the codes can be hidden in the picture - and retrieved by a technician at a later stage.

Videocrypt-your flexible friend?

Videocrypt can be used in a number of applications other than tv signals protection. They include:

Messaging, messages can be transmitted to individual subscribers or to a group, so target messaging is now a potential. Messages like: "Satellite owners in LONDON call 081 XXX XXXX now for a great bargain".

Selling, sales over the air can be utilised with the unique identity number which verifies an owner and their registered address. Data can be matrixed with a user personality during ad-breaks to tailor-make the advertisement.

A unique transaction alphanumeric can be displayed on the TV screen, and the subscriber will telephone a given number and quote the alphanumeric - and the deal can then be completed in total security.

Scrambling

The majority of scrambling systems currently on the market are dependent on analogue processing circuitry, and it is a hard task to get a secure system without picture deterioration.

Videocrypt can encode and decode a picture without degradation.

The crux of the scrambling system evolves around a patented development of Active Line Rotation (Cut and Rotate principle).

Every line of the signal is cut at a number or points along its length, and this is chosen at random by a 60 bit psuedo random binary sequence generator (PRBS). As each cut point differs from the next the signal has no viewing value to an unauthorised recipient, but authorised recipients decoders recode the picture so that the true state of the unscrambled line is always first out for display.

The PRBS is re-seeded at times too, to enhance the security of the system even more.

Before this ALR process can take place, the decoder needs to be aware of the cut point on each of the transmitted lines, this is provided within the encryption process. Each decoder utilises an PRBS which reflects the characteristics of the system so that the two halfs can be synchronised and a viewable picture displayed.

Data is transmitted in a series of over-the-air packets, which looks like:

SYSTEM-----SMART or BLACKLIST

The system comprises of system data included Flat-Shamir identification information, on-screen display messages, fingerprinting and blacklisting data.

The smart card packet comprises of:

HEADER-----ENCRYPTED DATA-----CHECKSUM

The Videocrypt encryption system is based around a tightly-guarded secret which has defeated system hackers throughout the world. A final control algorithm is central to the systems security and this can be changed at will if the system has been hacked.

Complex calculations are performed within the system in order not to compromise its security.

But hackers who have attempted to hack the decoder will be disappointed - as there are no secrets held within the system.

Smart Cards

The smart card offers great flexibility to the programme controller and the viewer alike, and is the key to the Videocrypt system.

The Integrated circuits incorporated within the smart card have a lot of power and contain EPROM elements which are partially burned during their manufacture. The ICs are buried within the design to make the system harder to penetrate.

Smart card block diagram

```
   -------     -------     -------
   VCC  ->       - RAM -     - ROM -     -EPROM-
   -------     -------     -------
   ^           ^           ^
   TO AND FROM
   -------------------------------
GND ->        -    INTERNAL BUS            -
   -------------------------------
   TO AND FROM
   -------     -------     -------
   -8 BIT-     -ANTI -     -S/WRE-
RST ->        -CPU  -     -FRAUD-     -CNTRL-
   -    -    -DVCES-     -I/FCE-
   -------     -------     -------


   CLK        VPP          I/O
```

Over the air addressing

Algorithmic information is transmitted to the viewer over the air, encrypted within the Videocrypt system.

This data is transmitted within the Vertical Blanking Interval (VBI) and four lines are employed for active data and two others, one white and one black (for test purposes).

An application of Non Return To Zero (NRZ) with an constant energy spectrum maximises the systems characteristics.

Four picture-sustaining techniques are used to ensure a high quality picture. Bit interleaving, hamming codes, quadruple repetition and check sums are used within the process.

The system can cope with fringe reception areas and will still function correctly with high levels of noise.

Picture quality

Picture quality is paramount for any scrambling system and due to the standard being of a digital origin, integrity of the signal is maintained throughout the encryption and de-encryption process. Amplitude sampling is conducted by the decoder and a 14MHz internal clock ensures jitter-free pictures and unstable framing. A digitally derived Automatic Gain Control (AGC) is also included within the receiver.

Scrambling Sound

Videocrypt also has the capability of encrypting sound sources to enhance the security of premium events. To date this level of security has not been utilised by broadcasters.

The system of spectrum inversion renders the sounds received without authorisation worthless. Videocrypt transposes the frequencies transmitted and this in turn removed distortion of the sound.

Technical Data
(supplied by Thomson Consumer Electronics, 1991- subject to change)

VIDEOCRYPT BASEBAND DECODER
* Stand alone video decoder
* On screen display
* De emphasis switch
* Authorise button
* Integrated smart card reader
* Power indicator

PAL MODEL

Video input level	IV +/- 3dB flat and clamped
Baseband input level	250 mV +/- 3dB, unclamped level
measured at pre-emphasised transition frequency	
Suitable de-emphasis	CCIR 405-1
Video output level	IV p.p. into 75 ohms
Video bandwith	50Hz - 4.8 Mhz -3dB typical
Line tilt	<_ 1% typical
Luma/Chroma Delay	+/- 50nS typical
S/N ratio:	50dB typical weighted

CONNECTIONS

AV Peritel (Scart)

Audio loopthrough	Left and right
Pin 8	High with scrambled video input Low with clear video input
Pin 16	5v 50mA maximum for external modulator (OPTION)

MISCELLANEOUS

Standards	Designed to IEC 65
Operating Temperature Range	5-40 C
Mains Input	216-255 V AC 50 Hz
Power Consumption	15W
Weight	2.5Kg

VIDEOCRYPT ENCODER (PAL/SECAM/NTSC)

* 19" rack mounting
* Active line cut and rotate
* Twin or single scrambler
* Separate power supply
* Integrated cooling unit
* Data for control access in the VBI
* RS232 interface

Video input level	IV 75 ohm
Video output level	IV peak to peak +/- 2% 75 ohm
Line tilt	0.5% typical
Base line distortion	0.5% typical
Chrominance to luminance	3% typical
2T/Bar ratio	2% typical
Synchro level	1% typical
S/n ratio RMS weighted	>_ 67dB
Chrominance luminance:	
intermodulation	<_ 2%
differential gain	1% typical
differential phase	1" typical
luminance non-linearity	1% typical
chrominance/luminance delay	+/- 10nS typical
video bandwith at 3dB	>_ 5.8 Mhz
Output DC level	300 mV +/- 50 mV
Sampling frequency rejection	>- 50dB at 14 Mhz
Number of bits per sample	10

CONNECTIONS

Connections to security comp	RS232
Local VT100 terminal	ditto
Video in	BNC 75 ohm
Scrambled video out	BNC 75 ohm

MISC

Local terminal functions are to
show working parameters
give warnings
control local
remote
autonomous

Select scrambling mode
clear
free access
control access

Mains input low pass filtering
Audio scrambling using spectrum
inversion 0dB/600 ohm (optional)

ENDS

When the VideoCrypt system was launched, the press releases claimed that it was the most pirateproof system yet devised. Some of the people involved in the design of the system claimed that it would take billions of years to break the codes used by the system. The usual media journalists swallowed this hook line and sinker. The hackers knew otherwise.

The VideoCrypt system is the mainstay of the BSkyB satellite television empire. It is the means by which BSkyB makes its money from the subscribers. The basic theory is that they pay a subscription for the premium channels and they receive a smart card. This smart card, when inserted into the VideoCrypt decoder will allow the decoder to descramble the channels paid for. It is also possible for BSkyB to turn off the cards of those subscribers who have not paid.

Hacking scrambling systems such as VideoCrypt is a multi-million pound industry. Due to the present legal situation it is perfectly legal to hack a channel that originates outside the UK. However for someone in the UK to hack a UK originated channel is illegal. Such mere facts as illegality have never bothered pirates.

In the last few weeks the impossible has happened. The VideoCrypt system has been conclusively hacked. It is now possible to purchase a pirate smart card or chip which will allow the viewer to descramble Sky Movies Plus, The Movie Channel, Sky Gold, Sky Sports and TV Asia. The cost of this pirate card is œ99. The price in itself is lower than the subscription for the channels.

Other channels using the VideoCrypt system. Are worried. According to the latest reports, The Adult Channel and JSTV have been compromised as well. This means that all of the channels currently using the VideoCrypt system as a fee gathering system have just lost control of the market. It is now, well for the moment anyway.
a pirate's market.

This hack is, like all hacks, colourfully named. It is known as the "Ho Lee Fook" hack. The joke being that this is generally the exclamation uttered by people when told of the hack. There are two forms of the hack; a card and a chip.

The card version of the hack is about sixteen millimetres longer than the official BSkyB card. Essentially it is a single chip mounted on a printed circuit board that plugs directly into the VideoCrypt decoder's card socket. This is the more user-friendly version as it does not require any modification to the decoder.

The chip version does require some modification to the decoder. The official VideoCrypt name for the chip in the decoder is "The Verifier". This chip has to be removed and replaced with the pirate chip. The decoder will then decode the scrambled channels without the need for the BSkyB smart card.

The pirate cards and the chips are on sale. It is believed that a number of them are already in the UK. Indeed I received one, in a brown paper envelope, on June the eighth. It is still working.

The problem for BSkyB and other users of the VideoCrypt system is not one of containment. Things have progressed too far for that. The problem is more serious. Unless they can come up with a quick fix for the system that will render the Ho Lee Fook hack inactive, they have to replace the smart cards.

BSkyB initially set out to replace their smart cards every three months. This continual update was, so the theory went, meant to deter hackers from trying to hack the system. Fiscal reality has a crushing effect of such business school theories.

VideoCrypt suffered its first real disaster when someone discovered that by limiting the programming voltage to the card, it was possible to stop the card being switched off. This hack was known as the "Infinite Lives" hack. It was an old computer term for a modification to a games program that gave the player unlimited lives. Since BSkyB could not turn off the cards it seemed an apt name. This hack was followed by a new issue or batch of cards. The "Infinite Lives" hack did not work on the new cards but a new hack did.

The KENtucky Fried Chip upped the ante. It was the first time that the actual internal operation of the VideoCrypt decoder was interfered with. It was a rewritten "Verifier" chip that was programmed to stop the cards being turned off. It did not work at full efficiency so it was not marketed by the pirates. After this hack, BSkyB issued a new batch of cards which was more resilient to this hack.

The current card issue is issue 07. The Ho Lee Fook hack is working on this batch. If BSkyB introduce issue 08 cards, then there is the possibility of the hack ceasing to work. At this stage there is the terrible spectre of the hack being updated to work with the 08 cards. It is the thing of which BSkyB's nightmares are made of.

The issue of new card batches occurs mainly in Spring or Autumn. A Summer launch of the new 08 cards would be unusual. As VideoCrypt will be going to a tiered channel structure in the Autumn, it would seem that they have planned an Autumn update. The Ho Lee Fook hack may force them to bring their plans forward by some three months or so.

The confidence in a system is not based on how well a system repels hacks but rather on how well a system recovers from hacks. This will be a true test of the VideoCrypt system and its smart card based philosophy. The philosophy is that of the detachable secure controller. Basically what this means is that if the system is hacked then all that needs to be done to stop the hack is to issue a new card.

The effects on the confidence of present and prospective users of VideoCrypt is more difficult to gauge. The smart card is the core of the VideoCrypt system. Seeing it replaced by a pirate smart card contradicts every claim made in favour of VideoCrypt. It was not supposed to be possible. One thing is certain, channels will now have to look at a scrambling system as only being a temporary form of protection that has to be frequently updated. Failure to do so will be fatal.

John McCormac
Author of "European Scrambling Systems 3" ISBN 1-873556-02-0
Editor of Hack Watch News.---

*** Latest ***

There is no such thing as coincidence - or is there? On the day that the film "Sneakers" was released on video, I received an actual working hack for the scrambled Sky channels. The film "Sneakers" is about events surrounding a piece of equipment that can hack any cryptosystem. The piece of equipment that I received is essentially a chip that can hack the Sky VideoCrypt channels.
This latest hack on the VideoCrypt system has been labelled the "Ho Lee Fook" hack. The reason for this name is more to do with people's reaction to the hack rather than its origin, which incidentally is Central Europe.
This is perhaps the most dangerous hack to have occurred on VideoCrypt - it replaces the smart card. In effect it is a new smart card that gives access to all the Sky channels. Of course the problem for Sky is that it is not a genuine Sky card.

The card is approximately sixteen millimetres longer than the official Sky card. It is a blue printed circuit with a single surface mount chip, and five connector pads. The identification numbers on the chip have been scrubbed.
The standard check for a card of this nature is to look for a wafer from an official smart card. In the early days, a fairly common scam

was to take the chip and connector pad from a valid Sky card, trim away the plastic and then put the chip in a DIL header. The DIL header would then be blobbed in a lump of black resin so that it looked like an IC.
The decoder would then have its card reader replaced with an ordinary DIL IC socket. Then the decoder and chip would be shown or sold to some unsuspecting, if greedy, punter.
The chip appeared to be real, with no wafer underneath the body of the chip. The actual stubs of the chip die were just visible at the end of the chip. It was a genuine chip.

It has been working steadily for the last few days and there appears to have been no kill messages sent to it. If it had been a direct clone, Sky would have been able to kill it over the air - or would they?
Since the people who developed this hack obviously understand the operation of the over the air addressing, they may well have designed a filter to stop the kill message from having any effect of the pirate card. There are of course more devastating implications here. The card itself may only contain the data and algorithms necessary to descramble the signals.
The chip version of this hack is based on the 8752. This Ho Lee Fook chip will replace the official 8052 in the decoder. A selling price of ninety nine pounds has been mentioned in Germany.

Nobody is sure what the people in News Datacom are doing about this hack. Sky are more than likely very upset that someone has hacked their pirateproof system yet again. This is the fifth hack and the image of a pirateproof system now only exists in the minds of PR people.

```
                  ------------------------
                  ULTRA-SONIC JAMMER PLANS
                  ------------------------



                        UNIT ONE

                          24 MH
                       ------------ CHOKE
                       ------------
         +---------------/\/\/\/\/\/\---------------+
         :                  :                :
         :                  :                :
         :                  + 12VDC                 :
         :       .002                  .002      :
         +--------) |----------+-----------) :------+
         :                  :                :
```

```
:              GND                :
:    .001                       :
+------) |----+-------+--------+          :
:         :     :      :        :
:         \     B      \         :
:      500 /     / \     / 120K     :
:         \    E   C     \        :
:         :    : 1 :     :        :
:   GND------+-----+   +------+---/\/\----+
:                        2.2K    :
:                              :
+------) |------------+-----------) |------+
    10PF         :         .1NF
                 :
     *           +-------+
    5NF          :       :
+------) |------+     B      /
:            :    / \     \ 120K
:            :   E   C     /
:   200      :   : 2 :    :    3K    (B)
+-----/\/\------+---+   +-----+----/\/\----+ 12VDC
:                           ^
:   4.7K                    :  <-- POTENTIOMETER
+-----/\/\------------+--------------+
:              :
:              B
:             / \
:            E   C
:    470       : 3 :            (A)
+-----/\/\----------+   +------------------+ 12VDC
:            :
:            :
:    1*        :
+---TWEETER---) |---+
    : :   1000PF
   /___\
```

```
          ----------------
          : EXPLANATIONS :
          ----------------


/\/\ = Resistor    --) |-- = Capacitor    --- = Wire

 +   = Connection   /\/\   = Varible Resistor
                     ^
                     :
 :
 B
/ \  = NPN TRANSISTOR   B=Base, E=Emeter, and C=Collector
E   C
:   :
     1. HEP 52
```

2. HEP 52
3. 2N2338

---

* Capacitor may have to be increased to prevent degenerative feedback.
1* Tweeter should be Mustang "Sphericon" or other capable of 40000Hz.

UNIT TWO

```
                  +      120 VAC       +
                  :                    :
                  :                    :
                  :                    +
                  :                     \ ON/OFF SWITCH
                  :                    +
                  :                    :
                  +--\/\/\/\/\/\/\/--+
                     ----------------
                     ----------------    STEP DOWN TRANSFORMER
                     /\/\/\/\/\/\/\
          +-----------+                +----------+
          :                                       :
          :               12 VDC                  :
          :                                       :
          :                                       :
   +------ : ------------------+------------------ : ------+
   :      :                   :                   :       :
   :      :                   :                   :       :
   :      :                  / \                  :       :
   :      :    BRIDGE       /   \                 :       :
   :      :   RECTIFIER    /     \                :       :
   :      :               /  MOT  \               :       :
   :      +--------------+   MDA   +--------------+       :
   :                      \ 970-1 /                       :
   :                       \     /                        :
   :                        \   /                         :
   :                         \ /                          :
   :     1000NF               :              1000NF       :
   +-------) |----------------+--------+------| (---------+
   :                          :        :                  :
   :                          :        :                  :
   :                          \        \                  :
   :          1 OHM  10 WATT  /        /  1 OHM  10 WATT  :
   :                          \        \                  :
   :                          :        :                  :
   :         1000NF           :        :     1000NF       :
   +-----------) |-------------+        +------) |---------+
   :                          :        :                  :
   :                          :        :                  :
   :                          :        :                  :
   :                          :        :                  :
   +-------GND                :        :      GND--------+
                 :     :
                 :     :
                 :     :
                 :     :
      PLUS 12 FOR (B)  +     +  PLUS 12 FOR (A)
```

NOTICE - Output wires from transformer do NOT connect with overlapped wires.

NOTES:

The two top units must be constructed separately. Unit 1 is tuned by adjusting the choke to about 500 to 1000 cycles apart (this will be somewhere around 22,000 cycles - above human hearing.) Both units use common power supply, but should be electrostatically isolated from each other. The speaker must be seperated by several feet, or sonically seperated. The output is controlled by adjusting the 3K pot. When adjusted correctly it will cause ALL (including telephones, hearing aids, tape recorders, bugs, etc.) microphones to squeal at the difference in their frequencies. This will render useless all mics in the vicinity. Aim upward and let sound reflect from ceiling.

```
                ------------------------
                ULTRA-SONIC JAMMER PLANS
                ------------------------



                     UNIT ONE

                      24 MH
                   ------------ CHOKE
                   ------------
        +---------------/\/\/\/\/\/\---------------+
        :               :              :
        :               :              :
        :               + 12VDC              :
        :      .002               .002     :
        +--------) |----------+-----------) :------+
        :               :              :
        :              GND                  :
        :    .001                        :
        +------) |----+-------+--------+          :
        :          :     :      :       :
        :          \     B       \       :
        :       500 /     / \     / 120K      :
        :          \    E   C     \        :
```

```
:          :    : 1 :     :         :
:   GND------+-----+   +------+---/\/\----+
:                          2.2K    :
:                                  :
+------) |-----------+-----------) |------+
     10PF         :         .1NF
                :
      *          +-------+
     5NF          :     :
+------) |------+    B      /
:            :   / \     \ 120K
:            :   E   C    /
:    200      :   : 2 :    :    3K    (B)
+-----/\/\------+---+   +-----+----/\/\----+ 12VDC
:                             ^
:    4.7K                     :  <-- POTENTIOMETER
+-----/\/\------------+--------------+
:                 :
:                 B
:                / \
:               E   C
:     470        : 3 :              (A)
+-----/\/\----------+   +------------------+ 12VDC
:               :
:               :
:     1*         :
+---TWEETER---) |---+
    : :   1000PF
   /___\
```

```
                ----------------
                : EXPLANATIONS :
                ----------------


 /\/\ = Resistor    --) |-- = Capacitor    --- = Wire

  +   = Connection   /\/\   = Varible Resistor
                      ^
                      :
 :
 B
/ \  = NPN TRANSISTOR   B=Base, E=Emeter, and C=Collector
E   C
:   :
      1. HEP 52
      2. HEP 52
      3. 2N2338
```

* Capacitor may have to be increased to prevent degenerative feedback.

1* Tweeter should be Mustang "Sphericon" or other capable of 40000Hz.

```
                    UNIT TWO


                +      120 VAC       +
                :                    :
                :                    :
                :                    +
                :                     \ ON/OFF SWITCH
                :                    +
                :                    :
                +--\/\/\/\/\/\/\/\/--+
                  ----------------
                  ----------------    STEP DOWN TRANSFORMER
                  /\/\/\/\/\/\/\/\
         +-----------+                +----------+
         :                                    :
         :                12 VDC              :
         :                                    :
         :                                    :
   +------ : ------------------+------------------ : ------+
   :     :                 :                  :       :
   :     :                 :                  :       :
   :     :                / \                 :       :
   :     :   BRIDGE      /   \                 :       :
   :     :   RECTIFIER  /     \                :       :
   :     :             /  MOT  \              :       :
   :     +--------------+   MDA   +--------------+       :
   :                   \ 970-1 /                     :
   :                    \     /                      :
   :                     \   /                       :
   :                      \ /                        :
   :     1000NF              :             1000NF      :
   +-------) |-----------------+--------+------| (---------+
   :                       :       :                 :
   :                       :       :                 :
   :                       \       \                 :
   :          1 OHM  10 WATT  /       /  1 OHM  10 WATT  :
   :                       \       \                 :
   :                       :       :                 :
   :         1000NF          :       :     1000NF      :
   +-----------) |-------------+        +------) |---------+
   :                       :       :                 :
   :                       :       :                 :
   :                       :       :                 :
   :                       :       :                 :
   +-------GND               :       :      GND--------+
                           :       :
                           :       :
                           :       :
                           :       :
          PLUS 12 FOR (B)  +       +  PLUS 12 FOR (A)
```

NOTICE - Output wires from transformer do NOT connect with overlapped wires.

NOTES:

The two top units must be constructed separately. Unit 1 is tuned by adjusting the choke to about 500 to 1000 cycles apart (this will be somewhere around 22,000 cycles - above human hearing.) Both units use common power supply, but should be electrostatically isolated from each other. The speaker must be seperated by several feet, or sonically seperated. The output is controlled by adjusting the 3K pot. When adjusted correctly it will cause ALL (including telephones, hearing aids, tape recorders, bugs, etc.) microphones to squeal at the difference in their frequencies. This will render useless all mics in the vicinity. Aim upward and let sound reflect from ceiling.

** HOW TO MAKE A STUN GUN! **

So you want to ZaaaaaaP the shit out of someone. Well I have the thing just for you. It delivers a nice Shock of 75,000 Volts and causes muscle spasms. A word of caution don't try this on your self (Dumb Shit). Well you be need'n to go down to your local RADIO-SHACK. Yes that is what I said RADIO-SHACK where they sell shitty computers. Just for a joke tell'em you want to buy a TANDY 2000 to use for a clock (HA! HA!) , and watch'em turn red. Then say "just kidding(dick) ", under your breath of course. Well enough of that shit, Here is what you need.

PARTS
=====
All resistors are 1/2 watt.Abbrv. as R1 or R2.

R1 & R2 100,000 ohm's resistors!
R3 & R4 500,000 ohm's resistors!

DIODES:D1-D4
Use a 75 PIV BRIDGE RECTIFIER or 4 1N9004's 300 VOLTS.

Capacitors:
C1&C2 4700uF electrolytic

TR1-STEP UP TRANSFORMER 55 uH AUDIO
----
2 250 volt AC DPST switch

A 9volt RECHARGEABLE/100 volt Neon lamp =L

A 9volt battery clip/MALE-FEMALE RCA JACKS

Some perf board,wire,solder

```
---------------------------------------------
      9volts in
 -               +
 / to RCA JACK      /
|---* *-------------|       Use RCA JACK TO HOOK TO A RECHARGER.
|   sw2            |       Run JACK FROM 9V.
|----|<-----|<------|
|    d1     d2      |       When battery runs down Recharge it!
|----|<-----|<------|
|    d3     d4      |
|                  |
\                  /
/ R1               \ R2
\                  /
|  +               |
|----|(-------------|
|    c1            |
\                  \
/                  /
\                  \
| R3    -          | R4
|----|(-------------|
|    c2            L Neon charge light/ Push sw1 to fire when light is on
|/                 |
*   *---------|     |
 sw1          |     |
             +  n  -
             =======
             /\/\/\/ TR1
             =======
   |     |  needles or prods
             |     |
            \|/   \|/
```

When this is built hold down sw2 until neon lamp lights. Then Stick "THE VICTIM" And press SW1 ,He will get a jolt. Well I hope you have fun. Just don't throw this into a swimming pool full of "VICTIMS"! If you do this then well You'll see!

Disclamer:
This is for Informational purposes only!!!

DURING THE PAST EIGHT YEARS, I HAVE BEEN HEAVILY INVOLVED WITH "BULLETIN BOARD" SYSTEMS RUNNING ON MICROS AND MAINFRAMES. I'D LIKE TO GIVE A FEW EXAMPLES OF THE DESTRUCTIVENESS OF MANY OF THESE "KIDS."

MOST HAVE PROBABLY HEARD OF OR CALLED AN RCP/M. FIVE YEARS AGO, I WROTE A SIMILAR TYPE SYSTEM FOR A TRS-80. THIS SOFTWARE RAN FOR 3.5 YEARS WITHOUT A PROBLEM. BUT NOW, AS MORE AND MORE POTENTIAL CRACKERS HAVE ACCESS TO COMMUNICATIONS EQUIPMENT, THIS SYSTEM HAS BEEN CRASHED REPEATEDLY.

WHEN I WAS BACK IN HIGH SCHOOL, THE BIG THING WAS TO FIND A BUG IN THE OS.
BUT, ONCE WE FOUND IT, INSTEAD OF USING IT TO KEEP THE SYSTEM FLAT ON ITS
BACK, WE DOCUMENTED IT AND SOMETIMES EVEN FIXED IT. DOESN'T SEEM LIKE THAT
IS THE CASE ANYMORE...

ON THIS SYSTEM, SOME CALLER BREAKS IN, DELETES ALL THE FILES, AND THEN
WRITES A PROGRAM WHICH KEEPS THE DRIVES SELECTED; THIS BURNS OUT THE
MOTORS
ON 5.25" DRIVES, ESPECIALLY WHEN THEY RUN ALL NIGHT. THIS WAS DONE SO
OFTEN, THE SYSTEM WAS BROUGHT DOWN FOR A LONG TIME (UNTIL A TRACE COULD BE
PUT ON THE DIAL-UP).

I RUN MY OWN SYSTEM AND PUBLISH SOFTWARE THAT TURNS A TRS-80 INTO A MAIL
AND MESSAGE SYSTEM. I HAVE SAT AND WATCHED CALLERS SYSTEMATICALLY
ATTACK
THE SYSTEM. THIS TAKES SEVERAL FORMS:

1) ALL COMMANDS, SERIES OF COMMANDS, AND OPTIONS ARE TRIED.

2) THE SYSTEM IS ASSAULTED WITH ALL MANNERS OF CONTROL SEQUENCES, TRYING TO
GET SOME UNEXPECTED RESULT.

3) I HAVE EVEN SEEM SOMEONE DROP AND THEN RE-INITIATE CARRIER TO SEE IF
THEY COULD GET SOMEWHERE.

IF THAT DOESN'T WORK, THEY BEGIN TO CRACK PASSWORDS. THEY KNOW WHAT THEY
ARE
DOING... IN ONE CASE, I WATCHED AS SOMEONE WENT THROUGH WHAT LOOKED LIKE
THE
BEGINNING OF THE WEBSTER'S DICTIONARY TRYING TO GET SUPERUSER STATUS. SINCE
MOST PEOPLE USE WORDS, NOT A BAD IDEA, RIGHT? LESS INTELLIGENT ONES START
WITH
A AND JUST TRY AND TRY AND TRY.

OH, BY THE WAY, THEY ARE DEFINITELY USING AUTO-DIAL MODEMS AND SOFTWARE TO
DO THIS.

IF ALL ELSE FAILS, THEY SIMPLY TIE UP THE SYSTEM. THEY CHOOSE THE MOST
OBVIOUSLY DISK INTENSIVE COMMAND, AND EXECUTE IT AGAIN AND AGAIN. SINCE
MANY
SYSTEMS ONLY TIMEOUT AFTER INACTIVITY, THIS COULD TIE UP THE SYSTEM FOR
MANY
HOURS (NOT TO MENTION THE WEAR AND TEAR ON THE EQUIPMENT).

THESE LITTLE BASTARDS CERTAINLY AREN'T DOING ANYTHING CONSTRUCTIVE.

SEVEN YEARS AGO, I CALLED UP MIT-MC AND GOT A TOURIST ACCOUNT WHICH I KEPT
FOR THREE YEARS UNTIL I GOT AN AUTHORIZED ONE. IT WAS A FREE ACCOUNT ON
AN
OPEN SYSTEM; THE ONLY STRINGS WERE THAT I USE IT AFTER HOURS AND NOT TIE UP
TOO
MANY RESOURCES. BUT THINGS HAVE CHANGED. YOU CAN'T HAVE TOTALLY OPEN
SYSTEMS
ANYMORE WITHOUT MANY PRECAUTIONS AND ALMOST CONSTANT SUPERVISION.

FOR EXAMPLE, I HAVE HAD TO ADD MANY SECURITY FEATURES TO THESE SMALL SYSTEMS:

1) THREE ATTEMPTS AND YOU LOSE THE CONNECTION. NINE ILLEGAL ATTEMPTS AT A USERNAME WITHOUT A CORRECT LOGIN CAUSES A SUSPENSION . ANYONE TRYING TO LOGIN UNDER THAT NAME IS IMMEDIATELY SUSPENDED (WITH SOME EXCEPTIONS).

2) CONNECTION LIMITED USE.

3) APPLICATION PROCESS REVIEWED BY SYSOP BEFORE SOMEONE CAN USE ALL FEATURES, OR EVEN USE THE SYSTEM.

4) ISOLATE THE USER COMPLETELY FROM ALL OPERATING SYSTEM FUNCTIONS, EVEN TO THE POINT OF MODIFYING THE DOS TO HANG OR RESET WHEN NECESSARY.

I DO HAVE ONE LITTLE "JOKE" UP MY SLEEVE. THERE IS AN ACCOUNT ON THESE SYSTEMS CALLED SYSOP. NOW, IF I WAS GOING TO BREAK IN, THAT IS WHERE I WOULD START. I'VE PUT A LITTLE PATCH INTO MY HOST. AFTER 39 INCORRECT TRIES ON THAT ACCOUNT, IT ALLOWS THE CALLER THROUGH. HE GETS A WELCOME MESSAGE AND SYSOP COMMAND:. HE CAN RENUMBER MESSAGES, CHANGE THE DATE AND TIME, EVEN DELETE FROM THE DIRECTORY, CHANGE USERNAMES AND PASSWORDS. HE CAN DO ALL THE THINGS THAT A SYSOP CAN DO. OF COURSE, HE ISN'T *REALLY* DOING ANYTHING (HE HE HE!) AFTER, OH SAY, 10 MINUTES, OUTPUT STOPS. 24 LINEFEEDS ARE ISSUED AND THE FOLLOWING APPEARS (SLOWLY, AS IF FROM A TTY):

```
HELLO INTRUDER!  GEE, I WANT TO THANK YOU FOR HANGING AROUND FOR
THE PAST TEN MINUTES WHILE WE HAD A CHANCE TO TRACE YOUR CALL.  IT
IS TOO BAD THAT SOME PEOPLE JUST CAN'T LIVE RESPONSIBLY.  BUT, I
GUESS THAT IS THE REASON WE HAVE THE POLICE AND FBI, RIGHT?
[DISCONNECT]
```

I DON'T KNOW WHAT THE ANSWER IS, BUT I DO KNOWS THAT TREATING THIS TYPE OF BEHAVIOR CASUALLY MUST BE STOPPED. THERE WILL ALWAYS BE PEOPLE WHO WILL TRY TO CIRCUMVENT ALL SECURITY MEASURES, SOMETIMES OUT OF CURIOUSITY, BUT RECENTLY MORE OFTEN WITH THE INTENTION OF DOING SOMETHING DESTRUCTIVE.

IT'S TOO BAD THAT THE DAYS OF THE UNSECURED SYSTEMS IS COMING TO A CLOSE, BUT WITH HUNDREDS OF PEOPLE SCANNING THE EXCHANGES WITH THEIR AUTO-DIAL MODEMS LOOKING FOR CARRIERS, ARMED WITH 10 PAGES OF PIRATED MCI ACCESS CODES, WE DON'T HAVE MUCH CHOICE.

* How to Screw-over public utilities *

Part One : Telephone Company

The telephone company is probably the one that pays the most attention to what is going on out there. But they have messed on one major thing. THEY NEVER LOCK THE GREEN BOXES. The green boxes are the green boxes along the side of the road, with the Bell symbol on it. They have about 20 lines running out of them to different houses.

You can screw these boxes up very simply.....open it up, take a baseball bat, and smash that sucker to bits, and then close it again. This will most likely knock out all the lines connected to that box and the ones after that box. You should do this with the larger boxes with the double doors. (you need a hex wrench to open them).

Another way of doing this is to take two extra long pieces of stripped wire and wrap them around the separate lines of bolts in the box. This will cross all the lines in the neighborhood. Or else, just take one wire, and connect it inbetween ALL the bolts inside. Then the people will just get static when the pick up the fone.

You can steal a person's line, temporarily, by connecting their bolts, to yours, by two seperate wires. Then you can call out using their line. You have to make sure you take this off after about a night or so, because if Bell finds it, you're dead.

You could hook up the "Blotto Box" to the line out there.

You could intercept people's phone calls using the "Beige Box", and crank the people from their own line.

Part Two : Cable Company

These guys are as stupid as the phone co.. They leave their boxes unlocked too, and every cable wire has a tag with a number on it (address). Which means you can take out a certain person's cable, or else, steal their cable, and switch the tags on the wires. I haven't don't much with this, so goof with it...

Part Three : Street Utilities

This means the sewer people, and the paving people and that shit. Anyway, you guys can think up things do with it. These things are never really locked up, or anything, so just trash, mostly. Steal the signs too.

I have stolen many of those construction lights on the "horses", and sold them. good money.

Part Four : Water, Gas, Electricity

I don't know. I haven't ever fucked with these. Don't goof with the gas, though, or else you could end up on the moon. Electricity can be disabled, by chopping down a telephone pole or something. And Water can usually be knocked out, if there is a well there. I don't know all the kinds of wells, so goof with it...

Basics:

The basic reasons for trashing can vary, but are generally:

1> To obtain credit cards and/or carbons of credit cards.
2> To obtain any information that may be useful in the aid of phreaking.

When choosing a place to go trashing, one must keep in mind the following:

1> Location of dumpster
2> Security of property where dumpster is located
3> Type of trash that may be found

First, the location. You generally want to pick a place that is somewhat isolated, where there will not be a lot (preferably none) of people. To accomplish this, it is also best to do your trashing at night, as there will not likely be any employees at the location, and it is easier to hide and to not be seen by passers-by.

Second, the security. Places such as Telco buildings and large companies often have security guards on duty 24 hours, and often keep their dumpsters behind fences so as to discourage trespassing. Yes, you are trespassing when you start looking in someone's garbage can!!! So it is a good idea to check out the place you are going to trash for a day or so to get a feel for what kind of security they have. This way, you can avoid walking in blindly to some place and getting nabbed, or you can figure out where to park your car, or where to hide, or how to avoid the security (rent-a-cops).

Places such as department stores and banks most likely will not have any security for the outside of their buildings as they may not be able to afford it or may not anticipate trashers. Also, they may not have anything worth taking! So basically, check the place out before you just go and hit it.

Case in point. One night, my friend and I casually pulled into the parking lot of a Pacific Bell office, and before we knew what was happening, a security guard had a giant spotlight glaring down on us. We just casually made a u-turn as if we were just turning around to go the other way. (More on what to do if you get caught later).

Third, you must pick a place where you know there will be trash that is of use to you. Don't go trashing at some little deli, all you'll get is a bunch of rotten food! (Unless of course you know for a fact that the deli deals alot with credit cards). In searching for cards, pick places such as department stores or places that sell alot of expensive stuff.

Also, the local telephone company is, of course the place to go to find your basic phreaking info.

These have been some of the basics to keep in mind before you hit aplace. Now for some techniques to use to help increase the efficiency of your trashing endeavors.

Tips:

First of all, don't be afraid to actually go into the trash can. This is almost always necessary to reach the good stuff. Also, when you are ducking down inside a big dumpster, you cannot be seen by passing police cars or security guards who happen to waltz by.

Second, always have a lookout somewhere to keep an eye out for cops or employees who may be coming out to throw trash away. You may want to have some kind if signal so that if you have advanced warning of security, you can take evasive measures, like burying yourself in the trash.

Try not to spend too long in a given trash can. The longer you stay, the more you put yourself at risk of getting caught. This means that you cannot be too picky about what trash you take. There is plenty of time for that after you bail the scene with the goods. You may want to have a knife handy, however, to cut open boxes or bags, and a small flashlight is a good idea, although if possible, avoid using to much light or making too much noise, anything that could potentially attract someone.

A car is a good thing to have, if possible. This greatly increases the range of places you can hit in one night. It is a good idea, if you are accumulating alot of stuff, to stop somewhere secluded and well lit (like a school or empty shopping center) and sort out the trash so you can get rid of useless garbage like food, etc. Take all the useless garbage and dump it into another dumpster.

You may want to wear old clothes that can get messed up, and gloves are not a bad idea either, both to keep your hands clean, and to keep prints off of anything in case the place discovers what you have done.

What to do if you get caught:

This is perhaps the most important thing to keep in mind when trashing. What to do if you happen to be caught be someone and they want to know what you are doing.

If you can, run like hell! Only do this if you have a clean getaway and you think you can get away without too much problem. Keep in mind that trying to escape may only make your situation worse. Only run if it looks like they are gonna bust you.

In most cases, the people may just tell you to get out. They will probably ask you some dumb questions, like "What are you doing in the trash?" In this case, make up a story, like "Oh, my friend here threw a ball in here and I was looking for it." If the guard believes you, he will probably just tell you to get out with a strong warning.

If they are serious about nailing you, however, chances are you'll only get charged with trespassing, which is not a major crime. In any case, however, maintain an extremely high level of caution when trashing, and always remain calm and collected. You can usually bullshit your way out of just about anything if you play your cards right.

Hope this has helped you to gain some insight into how to go about gaining that valuable information you always wanted.

How to make a CO2 bomb

You will have to use up the cartridge first by either shooting it or whatever. With a nail, force a hole bigger so as to allow the powder and wick to fit in easily. Fill the cartridge with black powder and pack it in there real good by tapping the bottom of the cartridge on a hard surface (I said TAP not SLAM!). Insert a fuse. I recommend a good water-proof cannon fuse, or an m-80 type fuse, but firecracker fuses work, if you can run like a black man runs from the cops after raping a white girl.) Now, light it and run like hell! It does wonders for a row of mailboxes (like the ones in apartment complexes), a car (place under the gas tank), a picture window (place on window sill), a phone booth (place right under the phone), or any other devious place. This thing throws shrapnel, and can make quit a mess!! -Jolly Roger-

Touch Explosives

This is sort of a mild explosive, but it can be quite dangerous in large quantities. To make touch explosive (such as that found in a snap-n-pop, but more powerful), use this recipe:

- Mix iodine crystals into ammonia until the iodine crystals will not dissolve into the ammonia anymore. Pour off the excess ammonia and dry out the crystals on a baking sheet the same way as you dried the thermite (in other words, just let it sit overnight!).

- Be careful now because these crystals are now your touch explosive. Carefully wrap a bunch in paper (I mean carefully! Friction sets 'em off!) and throw them around.. pretty loud, huh? They are fun to put on someone's chair. Add a small fish sinker to them and they can be thrown a long distance (good for crowds, football games, concerts, etc.) Have fun! -Jolly Roger-

Letter Bombs

- You will first have to make a mild version of thermite. Use my recipe, but substitute iron fillings for rust.

- Mix the iron with aluminum fillings in a ratio of 75% aluminum to 25% iron. This mixture will burn violently in a closed space (such as an envelope). This bring us to our next ingredient...

- Go to the post office and buy an insulated (padded) envelope. You know, the type that is double layered... Seperate the layers and place the mild thermite in the main section, where the letter would go. Then place magnesium powder in the outer layer. There is your bomb!!

- Now to light it... this is the tricky part and hard to explain. Just keep experimenting until you get something that works. The fuse is just that touch explosive I have told you about in another one of my anarchy files. You might want to wrap it like a long cigarette and then place it at the top of the envelope in the outer layer (on top of the powdered magnesium). When the touch explosive is torn or even squeezed hard it will ignite the powdered magnesium (sort of a flash light) and then it will burn the mild thermite. If the thermite didn't blow up, it would at least burn the fuck out of your enemy (it does wonders on human flesh!).

NOW that is REVENGE!

Paint Bombs

To make a pain bomb you simply need a metal pain can with a refastenable lid, a nice bright color paint (green, pink, purple, or some gross color is perfect!), and a quantity of dry ice. Place the paint in the can and then drop the dry ice in. Quicky place the top on and then run like hell! With some testing you can time this to a science. It depends on the ratio of dry ice to paint to the size of the can to how full it is. If you are really pissed off at someone, you could place it on their doorstep, knock on the door, and then run!! Paint will fly all over the place HAHAHA!!

Smoke Bombs

Here is the recipe for one helluva smoke bomb!

4 parts sugar
6 parts potassium nitrate (Salt Peter)

Heat this mixture over a LOW flame until it melts, stirring well. Pour it into a future container and, before it solidifies, imbed a

few matches into the mixture to use as fuses. One pound of this
stuff will fill up a whole block with thick, white smoke!

BIC BALISTICS

INTRODUCTION:

I'm sure all of you are familiar with the Bic lighter, and I'm also sure you've tried to make the Bic Flamethrower at one time or another. Well... here's 2 more things you can do, First off is the Bic Rocket, and then the Bic Sparkler. Both work almost every time! Enjoy...

MATERIALS NEEDED:

2 or more Bic lighters (the big kind)
1 large open parkinglot with noncombustible material surrounding it

DIAGRAM:

```
       - NORMAL TOP AND SIDE -     - TOP AND SIDE, FLME BLOCKER REMOVED -

     Flame        |Flame Blocker   /=========\   Striker
          \   __   |   ___        //         \ /
           +_/__|<-+->|_+_|       ||M       +_O== <-+  .0.
          |:....|    |  |       ||A      |:....|  | |   |
          |  :  |    |  |       ||G      |  :  |  | |   |
          |  :  |    |  |       ||N      |  :  |  | |   |
 Fuel --->|  :  |<-+  |  |       ||I      |  :  |  | |   |
 Area 1   |  :  |  |  |  |       ||F      |  :  |  | |   |
          |__:__|  |  |___|       ||Y      |__:__|  | |___|
                 |             ||               |
                 |Fuel Area 2   //               |Fuel Valve
                              //
                __             //
     Striker--> /  \ <==========/
                \__/
                 .
        Flint--> I
                 #
       Spring--> #
```

PREPARATION:

First, hit the back side of the flame blocker against something and break it off. Take off the striker and get the spring and flint. Set them aside somewhere safe for later use. Next pull off the Fuel Valve, and put your fingure over the hole where the fuel comes out and shake it up. Leave your fingure on the hole.

LAUNCHING:

Find someplace where you can lay the lighter so the bottom faces up. Set it there, take the other lighter and light the rocket. It should burn just like it normally does, except the flame should be melting the plastic. It melts down to the fuel and... one of three things happens: It flies up into the air and explodes (usually about 10-20 feet up), Skips along the ground, or just explodes. It usually takes about 2 minutes for it to burn through the plastic. What every you do, don't go back to the lighter after it's been burning for more than 1 minute. And only go back if the flame went out!

BIC SPARKLER:

This isn't really a sparkler, but it sure is fun. Take the flint and the spring you set aside from the rocket and wrap the flint in the spring, like this, you pull the sprint, put the flint in the middle, like a plus sign, and then twist the spring once so it looks like this:

```
        Flint
          \
           ||
         ."||". <- Spring
        ."    ".
        "      "
```

Then hold it over the flame of the one lighter you have left until it starts to wrinkle up or get red. Then throw it against a wall and whoosh, sparks fly everywhere and there's a little char mark left on the wall.

CONCLUSION:

Enjoy these, they're lots of fun at parties when everyones drunk, the sparkler is really trippy then. They are both best at night, but good during the day as well. If you have any comments about this file, or suggestions for other files, leave me Feedback on my board (Shadows of Iga).

```
-----------------------------------------------------------------------
SHADOWS OF IGA...........150 MEGS............H/P/A............NO LONGER UP
ATLANTIS..................30 MEGS.............H/P.............804-355-7327
RIPCO.....................96 MEGS............H/P/A............312-528-5020
```

Making Explosives

This is the first of several reports on the building of explosives from commonly available materials. Some basic preparations are discussed in this report that I feel everyone has the right to know, despite itsdestructive nature. This report will be followed by others relating to the same subject.

Nitric Acid

The first thing we will discuss is the making of nitric acid. This is the one ingredient in many high explosive compounds that will be the most difficult to get your hands on. Some chemical companies sell this acid, but they insist on sending it motor freight, so it costs a bundle just to get the stuff to your house. Besides, if you ordered it, the government would know you had it and that is not good (They know just as well as I do what some ordinary guy wants to do with nitric). The first step in making the acid is to obtain the needed materials:

Battery acid	(Auto parts store)
Potassium nitrate	(Drug or fertilizer store)
Two glass jugs	(Juice jars, etc.)
Some rags	(Old clothes)
Some tape, NOT cellophane	(Duct tape, etc.)
Heat source	(Fire, Torch, etc.)
Water	(The faucet, dummy)

The first thing you need to do is to concentrate the battery acid (Sulpheric acid). To do this, just boil the acid until dense, white fumes appear, and no it is not fun to breath them (At ALL), so don't do it. You will need equal quantities of acid and granulated pottasium nitrate. Put the two chemicals into one jar and then press the other jar's mouth to the filled jar's mouth and wrap the joint with rags. Next, wrap the rag joint with tape. Then lay the assembly horizontal and raise the filled bottle above the empty bottle. Next, apply heat to the filled bottle until red fumes appear, then pour water over the empty bottle. Continue this procedure until there is you have about as much condensed liquid as the amount of sulpheric acid that you put in. Let the assembly cool, throw away the rags and tape and pour out the condensed liquid, this is your nitric acid.

Nitroglycerin

Nitroglycerin is one of the first popular high explosive compounds that came into use. It is very sensitive when frozen and causes headaches when absorbed through skin. Nitroglycerin (Nitro) is oxygen positive, which means it releases oxygen when it decomposes. It is also the explosive ingredient in dynamite. Nitroglycerin, like all high explosives requires a detonator to set it off, so don't run off and try to light it with a match. However, a good way to test any homemade explosive brew is to put a teeny drop on an anvil and then hit it with a hammer. The procedure to manufacture the oily substance is pretty easy to follow, but the directions must be followed exactly. Use a stainless steel thermometer to keep immersed in the nitration vessel at all times, and if at any time the temperature goes above 20 degrees C, or if red fumes

When and Where to Hit

First of all, you should only do this at 2-4 in the morning. That way mostly everyone is sleep. And will not look at the window and dial the police. Go to Big(Does not have to be , but it is advised) parking lots, with not too much light. Me and Byte Blaster hit were there were only house lights covering the parking lot.

Protection and Plans to Save Your Ass

You should have 2-3 people in the job.. You should always have one person not going in the cars, just looking out. But once you get skilled enough, you will now have to worry about a lookout.. It's always good to have a lookout though, because a cop can come anytime. Not after you , just maybe roming around..
If anyone comes out, sees you, or walking your way, rip what ever you are working on, and get the hell outta there. On one occasion Byte Blaster was working on getting a CB out of a car, and i saw a man and a woman, looking strait at us with bad intentions.

I yelling "PIGS"(Our Password) and he yanked the CB wires and we both got the hell out! The way we did it was, the person that knew or lived in that neighborhood(me) would run, and the visitor or non-knowing the town person

would follow. It's a good stratigy. Believe all that we say. Have we been
caught yet?

And when you are walking from parking lot to parking lot ,try not to let anyone see you(even if there just some old hags walking!) because they can be a witness and say, yes it is him!

Getting in Cars the Easy Way

Needed: One Bag, 2 people.

Now this is as easy as it gets, just go around pulling on door handles, and see who's a stupid ass to leave there door unlocked. Where we hit, it was over half the cars we tried! And before you open doors on a sharp looking car (Camaro,Porshe,Iroc-Z,ect.) look on the outside of the car for extra locks(to lock/unlock the alarm).

And if you see a blinking light by the dash board(looking through the window) don't open it, unless you wanna open it and run(Fer fun ya know!). I guess that's all?!? ok now to the next chapter.

Getting into Cars The More Advanced Way...

Needed Onle long thin piece of Metal, Or a Very strong Knife.
1 Coat Hanger
2 People.

Well we all now if you have somthing Valuable in the car you may lock it up, Unless your a Dumb ass, Anyway then this is why
advanced knowledge is needed to be known about the system in which cars lock,

(The Lock)
Well You dont need to know every thing about the lock (It could help But I'm in no postion to tell you but I can help you in getting in) Simply put to unlock a door you only have to lift a little bar with in the door.

Procedure

Ok, Take the coat hanger and just bend the hanger together so it is a long
it looks like so:

```
                     ######
                        #
                        #
                        #
     ######################################
```

Ok then once you at the car take the piece of metal and seperate the rubber from the window and then slide the coat hanger in. The object is to get the coat hanger's curl under the bar and then lift up to unlock the car Get it??? The bar is usally located right about 8 inches under the Lock Button.

Where to look and What to get.

 Well once in the car you want to search for these items..

(1) Radio-- Not hard to Find you would be surprised what pawnn shops Pay...

(2) Money-- Any kind of money helps search for Wallets coin Purses and etc,
Believe me in one night I got about 20 Dollars in Change. Search between
seats and In golve Compartment or somtimes there is space under the Radio.

(3) Keys-- Alot of people Leave there Phucking Keys in the car so
if you find them Phucking go, Me and Cracka once phucking went in a Ferrari.
Or they maybe house keys and you then can expand your
capabilities...

(4) Carbon Copys-- Yes they are here too. Alot of people go Shopping they
somtimes leave there Carbons in the car.

(5) Anything-- Believe me once your in Take any Phucking thing you want!!!!!

Closure

 Believe me Breaking into cars can be rewarding take a look at
what me and Cracka Got in one night...

One 20 Dollar FlashLight...
200 Dollar Camera
4 Packs of Ciggerates
One Ladys Watch
One Gold Mans watch
4 Corbon Copy's
50 Dollar Binoculers
A CheckBook
A Lighter
4 Pens
2 Batteries
A pair of SunGlasses (I liked them)
A CB
Keys to a Ferrrari
Weed Paper
5 150 Dollar Radios
and Last but not least
A little Pink Button (I Dont know how we got it)

When and Which houses to hit.

You will have to definantly have to hit a home where no one is home, unless
you

are a dumb ass, or you are a Serious murderer or something like that. The best way is to find out who is going on vacation, or who will be gone for the night...make sure you do this about 1-2 in the morning! No one should know who you are!

Breaking Into the House

As Byte Blaster and I have found to be a good Quanity in people is 2. Alot of people could give you away. There are a few techniques for breaking and entering the house. The way Byte Blaster and I figure is the safest and best way is what we call the "BWAR" Technique(Break Window and Run). Will We surely go over this technique with you. And make sure mostly everyone is inside and maybe sleep. Try not to make alot of noise while breaking in And don't walk around the area alot before you break&enter. This is what we call "Chicken Shit!". So go straight to it!
Here we will go over some of the techniques that we know for Breaking & Entering.

BWAR(Break Window And Run)

This is the far easiest,safest way(For Byte and I anyway!). First you find a side or rear window that you can break. Find a rock that you can throw through the window. And here's what you have to do...

1st) Make sure no one is looking.
2nd) Throw the rock through the side are rear window.
3rd) Run to a place were you can see if anyone comes outside to see what happen
4th) Look and see if someone comes out.
5th) Go home and chill for about a hour.
6th) Come back out and see if there are policemen or anything.
7th) Unlock the window through the hole you made with the rock.
8th) Open window and enter.

By the way... If the window is already unlocked, you can just go in when you first get there, just don't let anyone see you.
Don't rub your hand prints all over the window either.

You can also look under rugs, behind bushes ,ect.. for a spare key.

Other Ways to Gain entry.

Well, Now we will discuss using the Great invention of the Glass Cutter, I'am not going to tell you Who to use the glass cutter, Read the instuctions on the back, But Were to apply the glass cutter,
Ok you will need
2 People
1 glass Cutter
1 suction Cup
1 FlashLight

Procedure.

You will wanna cut in a Place were U will be able to unlock all of the locks witch are on the window, Take the Flashlight and Examine the Window and find What kind of Locks are keeping the Window Secure, Usally there are 2, One basic lock and 1 long piece of Wood or Metal to also Secure the Window, Place the suction cup in the middle of the Piece you are going to cutt then Cutt the window and once you have made the Complete Square or Circle Pull the glass free with the Suction cup, (Also Some Windows have maybe 2-3 layers for keeping in Heat, Or Cool Air,) So this Procedure may have to be Repeated several times. Once you have gotten through the glass reach in and unlock the window, (The hole should be cutt for your arm size, So you will be able to reach all locks) The Go in,

Smashing the Quiet way.

If the area of interest is somewhat actively populated, a rock thru the window just may not cut it... A nice little common sense trick to try is taping the window (this also works very nicely with automobiles). Duct tape is nice, but almost any should do. Apply well, such the it covers most of the area of the window (do and X with some strip going back & forth, up & down, etc). Then strike with a large blunt object (large in proportion to the window - a small smashing object on a large window will produce more noise than a larger smashing object would). The striking sound will still be heard, but the clattering glass (noisiest) will not since most of the pieces are stuck to the tape.

The Garage door opener.

This takes some electronics know-how, but will provide an easy way into any garage with an electric opener & can be lots of fun. Exact plans, or schematics have not been included but we'll go over the basic principle. Garage door openers have a special little code they use to open only that door. Make something that will scan thru all the different possibilities (like a lousy sequential code hacker). That way, within a few minutes the door will open, & all you have to do is turn on your snazy little device. Drive right in if you wish - load your van up with all the goods right inside !

Where to Look.

Well once you gain entry You want to make it Quick and Sweet, Ha, You will want to search

(1) Dresser Drawers
(2) Closets
(3) Jewerly Boxes (OF COURSE)
(4) Under Beds

(5) Basements
(6) And any where you want
(7) Common Sense should strike here!

But you really dont want to Stay in the house over 20 mins. Just in case someone Saw you or something...

Construction sites.

These are usually fun & but not quite as profitable as your regular breakin. It's not even a break in actually, since its all open. Regardless, there are lots of materials & many times equipment left laying around. Look when the house is on the stage of just about getting doors/windows & not developed very well (has that styrofoam looking shit where the walls will go). this is when the wiring usually goes in therefore lots of yet unused rolls of wire lying around for your electrical needs.

Also, in most all theft cases, police do will not fingerprint unless there is a suspect. But be careful regardless. Do not dress like a burgler. But do not dress like you! Disguise yourself so that you look like a normal person, other than yourself. Also, either sneak around so much that no one could possibly see you, or try to seem like a normal pedestrian. A jogger is usually a nice cover. As in any other criminal act, just use alot of common sense and everything should go down smoothly.

!!!!!!!!!!
!CrimeNet!
!!!!!!!!!!

Part II of Volumn II

-=SHOP LIFTING=-
----

written by:

The Beast
and
Cracka Jack

Good Places to Shop Lift

You should steal from open places that have many escapes (for if you get spotted!). Places like shopping centers, a By-it-self store. That means stores aren't in shopping centers/malls. I think you get the point there.

How To Act

Ok, you must remmeber these things while shop lifting:

```
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
      !1) Don't have a Guilty/Suspicious look on your face.  !
      !                                          !
      !2) Don't look in a hurry, act as you would if you were!
      !   just looking around.                           !
      !                                          !
      !3) Make sure that where ever you hide it, it is not   !
      !   noticable! Sometimes a piece of software will stick!
      !   out and you will not notice it until after you're  !
      !   caught!                                    !
      !                                          !
      !4) Don't stay in the store too long! Or else the      !
      !   employees start to wonder.                     !
      !                                          !
      !5) Don't shop lift at the same store all the time.    !
      !                                          !
      !6) Don't run or do anything that will attrack the     !
      !   attention of employees/guards.                 !
      !                                          !
      !7) Don't piss around. Get your shit quickly & casually!
      !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The people who are supposed to be in stores are shoppers. Therefore, you want to blend in so not to be noticed. Blending in requires you to seem like a shopper. If you're not quite exactly sure on the behavioral patterns of a shopper, spend some time observing them. Also, try acting odd or figity (while not attempting to lift anything) to see how employees react & to see how far you will have to go in your little act.

Thus, the biggest point is ACT LIKE A SHOPPER.

If You Get Caught?

Hmm, you messed up ,eh? Oh well...
There's 3 things you can try.

1) Act real sorry and tell the manager you didn't mean it
   and that you'll never do it again. Try to create some
   tears if possible. There's two things that may happen:

A: He can let you go free.
B: He can press charges & you can pay the fine, or smack him and run! But make
   sure you can get away!

2) Deny anything he says!

3) Sit there and pay the fine..

Authoritative figures (fascists!).

A) Store employees - These should present little problem with confrontations.
a
smooth bullshitter should be able to talk his way from
any
such persons. However, some could be bitchy since some
employees have to pay for whats stolen during their
shift.
Then just bs your way out.

B) Mall Rent-a-cops - These men are complete bastards who will try to make
the
smallest little thing into a major federal offense.
NOTE: Rent-a-cops are the big fatasses who roam the
malls with their walkie talkies & plastic sticks
(can't have real guns). Most are old & overweight so
you should be able to outrun them but they do have
radio but are so unorginzed it really doesn't matter.

C) Local cops - These are touchy. some are bastards like above, and others
are quite gullable. Use your best bullshitting here.

D) State cops - forget it! staties are bad news. they are almost completely
immune to even the best bullshitting. These guys are smart
and should never be underestimated. The best thing to do with
a state cop is to NEVER lie but try to make your actions sound
as good and innocent as possible. Since they see alot of
really
major violence/crimes/etc try to make your little mishap
sound
as innocent as possible. Throw yourself at their mercy & pray
they let you go somehow.

E) Feds - if you've gotten busted for something so big that these guys show
up,
get a lawyer...

Things to watch for.
----

1) Employees watching you. If you notice this, & you've got goods hidden
away,
try & get rid of them somehow. Or act like you're comparing similar
products
or like you have a question about that particular product.

2) Reflective looking balls in the ceiling. this are nasty since there aren't
always cameras inside, & if there is, you don't know where they're pointed.

3) Cameras & mirrors, naturally.

4) Undercover people or little kids. Little kids are simply amazed at
   shopplifters. They will not take their eyes off yo. This could lead to
   one squeeling, or simply making others aware that somethings not right
about   you thus attracting more unwanted attention.

```
\          |              |         |/|  |     E             |
/          |      5 5 5     |   |        |    o L x________     |
|          |              |   \        |   | A        |  - |
|          |   Integrated    |    / R2       |   | Y        |   -----
|____________7|     Circuit     |   \        _|__  |         LED   --- 9
|          |              |   /         /\  |          |   + |  v
|____________6|              |2___|      D2 /__\  |          |    |  o
|          |              |   |        |   |         A    |  l
|          |____________________|   |         |____|          |    |  t
|            |1    |5          ---        |              |    |
|      C1      |     |          --- Switch   |              |_____|
|_______| (______|______|______________|___________|
       +           |                              A= Alligator
                 -----        R2=10K ohms                 Clips
                  ---
                  - Ground (-)      ** note: no connection between pins
                                      3 & 4.
```

The bottom of the relay has five pins. The pins here are marked with an "x" or an "o" corresponding to the schematic:

```
                  ____________________
                 |                |
                 | x   o            |     RELAY SWITCH
                 |                |    (bottom base)
                 |                |
                 | N   o         x  |     N= not used
                 |___________________ |
```

The alligator clips should be attached to the breadboard using short pieces of wire.

The longer lead on the LED is the positive lead. Make sure you hook it up with the right polarity. Same rule goes for the capacitor.

The pins on the 555 IC are numbered from the top (side with paint & notch). On the left side the read DOWN as 1,2,3,4. On the right side the read DOWN 8,7,6,5.

TEST

Attach the two batteries and clip roach clips together, the LED will light. Press and hold the switch for 3 seconds. You should hear a click then the LED will go out. In a little while (depending on what capacitor and resistor size you use), you should hear another click and the LED will turn on again. If this doesn't happen, you phucked up! Check your circuit carefully.

USING DETONATOR

**** Read these instructions carefully before attempting this ****

If the TEST worked, the timer is ready to use. Attach two fresh batteries and connect the two roach clips. Allow time equivalent to your delay for the capactitor to charge. Now, press the switch until the LED goes out. Now, quickly but carefully attach the roach clips to the Solar Igniter that has been previously attached to your bomb. Then, get the phuck out of there!!! Once the time delay expires, the relay will open completing the second circuit and igniting the Solar Igniter.

Tech Note: The values of R1 and C1 determine the time delay. The greater these values, the longer the delay. The equation to determine time delay is as follows:

$$\text{Time (in seconds)} = \frac{\text{C1 (in farads) x R1 (in ohms)}}{6}$$

The value of C1 is in farads. Most capacitors are listed in microfarads. To use the formula, divide the number of microfarads by 1,000,000.

Example: If you use a 500 microfarad capacitor for C1 and a 10 megaohm resistor for R1, you would have a delay of 14 minutes (833 seconds).

NO.	INGREDIENTS	AMOUNT
#1	NG	32
	SODIUM NITRATE	28
	WOODMEAL	10
	AMMONIUM OXALATE	29
	GUNCOTTEN	1
#2	NG	24
	POTASSIUM NITRATE	9
	SODIUM NITATE	56
	WOODMEAL	9
	AMMONIUM OXALATE	2
#3	NG	35.5
	POTASSIUM NITRATE	44.5
	WOODMEAL	6
	GUNCOTTON	2.5
	VASELINE	5.5
	POWDERED CHARCOAL	6
#4	NG	25
	POTASSIUM NITRATE	26
	WOODMEAL	34
	BARIUM NITRATE	5
	STARCH	10
#5	NG	57
	POTASSIUM NITRATE	19
	WOODMEAL	9
	AMMONIUM OXALATE	12

	GUNCOTTON	3
#6	NG	18
	SODIUM NITRATE	70
	WOODMEAL	5.5
	POTASSIUM CHLORIDE	4.5
	CHALK	2
#7	NG	26
	WOODMEAL	40
	BARIUM NITRATE	32
	SODIUM CARBONATE	2
#8	NG	44
	WOODMEAL	12
	ANHYDROUS SODIUM SULFATE	44
#9	NG	24
	POTASSIUM NITRATE	32.5
	WOODMEAL	33.5
	AMMONIUM OXALATE	10
#10	NG	26
	POTASSIUM NITRATE	33
	WOODMEAL	41
#11	NG	15
	SODIUM NITRATE	62.9
	WOODMEAL	21.2
	SODIUM CARBONATE	.9
#12	NG	35
	SODIUM NITRATE	27
	WOODMEAL	10
	AMMONIUM OXALATE	1
#13	NG	32
	POTASSIUM NITRATE	27
	WOODMEAL	10
	AMMONIUM OXALATE	30
	GUNCOTTON	1
#14	NG	33
	WOODMEAL	10.3
	AMMONIUM OXALATE	29
	GUNCOTTON	.7
	POTASSIUM PERCHLORIDE	27
#15	NG	40
	SODIUM NITRATE	45
	WOODMEAL	15
#16	NG	47
	STARCH	50
	GUNCOTTON	3

#17 NG	30
SODIUM NITRATE	22.3
WOODMEAL	40.5
POTASSIUM CHLORIDE	7.2

#18 NG	50
SODIUM NITRATE	32.6
WOODMEAL	17
AMMONIUM OXALATE	.4

#19 NG	23
POTASSIUM NITRATE	27.5
WOODMEAL	37
AMMONIUM OXALATE	8
BARIUM NITRATE	4
CALCIUM CARBONATE	.5

HOUSEHOLD EQUIVALANTS FOR CHEMICLES

IT HAS COME TO MY ATTENTION THAT MANY OF THESE CHEMICLES ARE SOLE UNDER BRAND NAMES, OR HAVE HOUSEHOLD EQUIVALANTS. HERE IS A LIST THAT MIGHT HELP YOU OUT.

ACETIC ACID	VINEGAR
ALUMINUM OXIDE	ALUMIA
ALUMINUM POTASSIUM SULFATE	ALUM
ALUMINUM SULFATE	ALUM
AMMONIUM HYDROXIDE	AMMONIA
CARBON CARBONATE	CHALK
CALCIUM HYPOCHLORIDE	BLEACHING POWDER
CALCIUM OXIDE	LIME
CALCIUM SULFATE	PLASTER OF PARIS
CARBONIC ACID	SELTZER
CARBON TETRACHLORIDE	CLEANING FLUID
ETHYLENE DICHLORIDE	DUTCH FLUID
FERRIC OXIDE	IRON RUST
GLUCOSE	CORN SYRUP
GRAPHITE	PENCIL LEAD
HYDROCHLORIC ACID	MURIATIC ACID
HYDROGEN PEROXIDE	PEROXIDE
LEAD ACETATE	SUGAR OF LEAD
LEAD TETROOXIDE	RED LEAD
MAGNESIUM SILICATE	TALC
MAGNESIUM SULFATE	EPSOM SALTS
NAPHTHALENE	MOTHBALLS
PHENOL	CARBOLIC

	ACID
POTASSIUM BICARBONATE	CREAM OF TARTER
POTASSIUM CHROMIUM SULF.	CHROME ALUM
POTASSIUM NITRATE	SALTPETER
SODIUM DIOXIDE	SAND
SODIUM BICARBONATE	BAKING SODA
SODIUM BORATE	BORAX
SODIUM CARBONATE	WASHING SODA
SODIUM CHLORIDE	SALT
SODIUM HYDROXIDE	LYE
SODIUM SILICATE	WATER GLASS
SODIUM SULFATE	GLAUBER'S SALT
SODIUM THIOSULFATE	PHOTOGRAPHER HYPO
SULFERIC ACID	BATTERY ACID
SUCROSE	CANE SUGAR
ZINC CHLORIDE	TINNER'S FLUID

KEEP THIS LIST HANDY AT ALL TIMES. IF YOU CAN'T SEEM TO GET ONE OR MORE OF THE INGREDIENTS TRY ANOTHER ONE. IF YOU STILL CAN'T, YOU CAN ALWAYS BUY SMALL AMOUNTS FROM YOUR SCHOOL, OR MAYBE FROM VARIOUS CHEMICAL COMPANIES. WHEN YOU DO THAT, BE SURE TO SAY AS LITTLE AS POSSIBLE, IF DURING THE SCHOOL YEAR, AND THEY ASK, SAY IT'S FOR A EXPEREMENT FOR SCHOOL.

AGAIN, I HATE TO BORE YA, BUT BE SURE TO FOLLOW INSTRUCTIONS CAREFULLY. A SLIGHT ERROR CAN KILL YOU

Mixing Your own Flash Powder

It is easy to get a file on how to make salutes, or how to make "meal powder," but, in the files I've read, they just use the generic term "flash powder" to mean the explosive stuff in your fireworks.

There are 2 types of explosives. Type I uses a non-explosive flash powder. "How can this be?" you ask? Well, the retort from a type I explosive comes from the rupturing of the case, not from the detonation of the powder. But we've all lit off M-80s, which have only a flimsy casing, which couldn't possibly account for the loud, ear-ringing bang you get from one. That comes from a more powerful powder which explodes when lit. This is a type][explosive. Potassium and barium nitrate powders, as well as black powder are used in type I explosives. Potassium chlorate and perchlorate powders are used in type][explosives. The list below has formulas for both types.

Potassium perchlorate mixtures:
1- 50% potassium perchlorate
25% dark pyro aluminum
25% sulfur flour

2- 70% potassium perchlorate
30% black german aluminum

3- 50% potassium perchlorate
30% black antimony sulfide
20% sulfur flour

4- 75% potassium perchlorate
25% dark pyro aluminum

5- 60% potassium perchlorate
40% sulfur flour

Potassium chlorate mixtures (note 1)

1- 50% potassium chlorate
50% red arsenic sulfide

2- 60% potassium chlorate
25% sulfur flour
10% potassium nitrate
5% red arsenic sulfide

Barium/potassium nitrate (type I)

1- 50% potassium nitrate
30% sulfur flour
20% dark pyro aluminum

2- 50% potassium nitrate
50% 100 mesh magnesium

3- 60% potassium nitrate
30% sulfur flour
10% charcoal dust

4- 50% barium nitrate   (note 2)
50% 100 mesh magnesium

5- 50% strontium nitrate (note 2)
50% 100 mesh magnesium

note 1- Chlorate mixtures are EXTREMELY dangerous. Don't mix them unless you like playing russian roulette.

note 2- These mixtures give colored flashes.

Mixing fireworks is very dangerous, and, I personally would never, ever, not-in-a-million-years ever mix them. For all you sickos out there who do, I assume no responsibility for any damage you fiendishly cause, or any injury that results from the manufature or use of the explosives detailed here. This was for information purposes only, blah, blah, blah.

YOU WILL NEED:-

A metal can with a press on lid. Examples are paint cans, or Hershey's Coco or Nestle's Quik cans. The new paper cans will work too but they wear out fast.
A tank of acetylene or the ACETYLENE GENERATOR from the preceeding file in this series <FZFF03>.

THE SETUP/ASSEMBLY:-

Drill or poke a small hole in the middle of the bottom of the metal can of 1/16" or less, diameter. Drill or poke a similar hole in the middle of the lid of the can. Put a piece of waterproof tape (like black electricians tape) over the outside of each hole.

USING IT:-

The easiest way to safely load the "Canon" is to begin by filling it with water and then using it in a collection trough (Like the one shown in FZFF03; Acetylene Gas). The bubbler tube can be connected to an acetylene tank such as on a welders torch, or the Acetylene Generator or bags of acetylene filled with the Generator shown in FZFF03. Once the can is full of gas (after the water has all drained out and bubbles start coming from under-neath the inverted can, press on the lid, and leave the tape in place.

IN PRINCIPLE:-

Once you take the <NOW LOADED> "Canon" to where you want to use it, by setting the can on something that will keep it off the ground and is ventillated underneath, countdown can be started. Remove the tape from both holes. Since Acetylene is lighter than air, air will begin entering the bottom hole as acetylene floats out the top. The flow is just about right to make a lantern flame above the exit hole at the top. Promptly light the top hole of the can and and get back, deliberately, as you will have several minutes to wait. (The time depends on the size of the can you use and the size of the pinholes you put in it.)

At the beginning, the can contains and vents only acetylene so that only above the can can it get enough air to burn, and only the gas which has exited is flamable. As air comes in the bottom, though, it begins to mix with the gas inside the can so that the mixture becomes increasingly activated with oxygen. Eventually the air level will reach its Flash Ratio, and the flame from the top of the can will move down inside, igniting all the acetylene that remains inside the can AT ONCE, and the "Canon" GOES OFF.

FIRING PHILOSOPHIES:-

Straight off you will see that you have a choice of setting off the shot with the lid up (to shoot the lid) or the lid down (to shoot the can) into the air. Also, because the fuse flame is sensitive to wind, you may want to fashion a chimney (or "Barrel") out of another can, a roll of linoleum or formica, or a length of PVC pipe of suitable diameter. This has two additional advantages beyond keeping the flame lighted, in that it dramatically enhances the BOOM, but also improves your control over the direction of the projectile ejected.

By loading many canisters with their holes taped, before hand, you then have yourself an easy reloader, cartridge fashion.

Another variation is to put the pinholes on opposite sides of the metal can and then mounting it in the "Barrel" horizontally. In this case, a backstop is needed and the chimney cannot be part of the "Barrel".

Some of my best shots have been 5 gal ice cream carton or hat box One-Shotters, filled dry from an acetylene tank at a wide setting. Because of the uncertainty of this fill method, these canons were lit with sparklers on the end of a 12 foot pole.

This kind of canon readily lends itself to loudness, altitude and distance competitions, since it's all hand made.

THE TERRORIST'S HANDBOOK

1.0   INTRODUCTION

Gunzenbomz Pyro-Technologies, a division of Chaos Industries (CHAOS), is proud to present this first edition of The Terrorist's Handbook. First and foremost, let it be stated that Chaos Industries assumes no responsibilities for any misuse of the information presented in this publication. The purpose of this is to show the many techniques and methods used by those people in this and other countries who employ terror as a means to political and social goals.The techniques herein can be obtained from public libraries, and can usually be carried out by a terrorist with minimal equipment. This makes one all the more frightened, since any lunatic or social deviant could obtain this information,and use it against anyone. The processes and techniques herein SHOULD NOT BE CARRIED OUT UNDER ANY CIRCUMSTANCES!! SERIOUS HARM OR DEATH COULD OCCUR FROM ATTEMPTING TO PERFORM ANY OF THE METHODS IN THIS PUBLICATION. THIS IS MERELY FOR READING ENJOYMENT, AND IS NOT INTENDED FOR ACTUAL USE!!Gunzenbomz Pyro-Technologies feels that it is important that everyone has some idea of just how easy it is for a terrorist to perform acts of terror; that is the reason for the existence of this publication.

1.1 Table of Contents

2.0 BUYING EXPLOSIVES AND PROPELLANTS

Almost any city or town of reasonable size has a gun store anda pharmacy. These are two of the places that potential terrorists visit inorder to purchase explosive material. All that one has to do is know somethingabout the non-explosive uses of the materials. Black powder, for example,is used in blackpowder firearms. It comes in varying "grades", with eachdifferent grade being a slightly different size. The grade of black powderdepends on what the calibre of the gun that it is used in; a fine grade ofpowder could burn too fast in the wrong caliber weapon. The rule is:the smaller the grade, the faster the burn rate of the powder.

2.01   BLACK POWDER

Black powder is generally available in three grades. As stated before,the smaller the grade, the faster the powder burns. Burn rate is extremelyimportant in bombs. Since an explosion is a rapid increase of gas volume ina confined environment, to make an explosion, a quick-burning powder isdesirable. The three common grades of black powder are listed below, alongwith the usual bore width (calibre) of what they are used in. Generally,the fastest burning powder, the FFF grade is desirable. However, the othergrades and uses are listed below:

GRADE	BORE WIDTH	EXAMPLE OF GUN
F	.50 or greater	model cannon; some rifles
FF	.36 - .50	large pistols; small rifles
FFF	.36 or smaller	pistols; derringers

The FFF grade is the fastest burning, because the smaller grade has more surface area or burning surface exposed to the flame front. The larger grades also have uses which will be discussed later. The price range ofblack powder, per pound, is about $8.50 - $9.00. The price is not affected by the grade, and so one saves oneself time and work if one buys the finer grade of powder. The major problems with black powder are that it can be ignited accidentally by static electricity, and that it has a tendency to absorb moisture from the air. To safely crush it, a bomber would use a plastic spoon and a wooden salad bowl. Taking a small pile at a time, he or she would apply pressure to the powder through the spoon and rub it in a series of strokes or circles, but not too hard. It is fine enough to use when it is about as fine as flour. The fineness, however, is dependant on what type of device one wishes to make; obviously, it would be impracticle to crush enough powder to fill a 1 foot by 4 inch radius pipe. Anyone can purchase black powder, since anyone can own black powder firearms in America.

2.02   PYRODEX

Pyrodex is a synthetic powder that is used like black powder. It comes in the same grades, but it is more expensive per pound. However, a one pound container of pyrodex contains more material by volume than a pound of blackpowder. It is much easier to crush to a very fine powder than black powder, and it is considerably safer and more reliable. This is because it will not be set off by static electricity, as black can be, and it is less inclined to absorb moisture. It costs about $10.00 per pound. It can be crushed in the same manner as black powder, or it can be dissolved in boiling water and dried.

2.03 ROCKET ENGINE POWDER

One of the most exciting hobbies nowadays is model rocketry. Estes is the largest producer of model rocket kits and engines. Rocket engines are composed of a single large grain of propellant. This grain is surrounded by a fairly heavy cardboard tubing. One gets the propellant by slitting the tube lengthwise, and unwrapping it like a paper towel roll. When this is done, the grey fire clay at either end of the propellant grain must be removed. This is usually done gently with a plastic or brass knife. The material is exceptionally hard, and must be crushed to be used. By gripping the grain on the widest setting on a set of pliers, and putting the grain and powder in a plastic bag,the powder will not break apart and shatter all over. This should be done to all the large chunks of powder, and then it should be crushed like black powder.Rocket engines come in various sizes, ranging from 1/4 A - 2T to the incredibly powerful D engines. The larger the engine, the more expensive. D engines come in packages of three, and cost about $5.00 per package. Rocket engines are perhaps the single most useful item sold in stores to a terrorist, since they can be used as is, or can be cannibalized for their explosive powder.

2.04 RIFLE/SHOTGUN POWDER

Rifle powder and shotgun powder are really the same from a practicle standpoint. They are both nitrocellulose based propellants. They will be referred to as gunpowder in all future references. Gunpowder is made by the action of concentrated nitric and sulfuric acid upon cotton. This material is then dissolved by solvents and then reformed in the desired grain size. When dealing with gunpowder, the grain size is not nearly as important as that of black powder. Both large and small grained gunpowder burn fairly slowly compared to black powder when unconfined, but when it is confined, gunpowder burns both hotter and with more gaseous expansion, producing more pressure. Therefore, the grinding process that is often necessary for other propellants is not necessary for gunpowder. Gunpowder costs about $9.00 per pound. Any idiot can buy it, since there are no restrictions on rifles or shotguns in the U.S.

2.05 FLASH POWDER

Flash powder is a mixture of powdered zirconium metal and various oxidizers. It is extremely sensitive to heat or sparks, and should be treated with more care than black powder, with which it should NEVER be mixed. It is sold in small containers which must be mixed and shaken before use. It is very finely powdered, and is available in three speeds: fast, medium, and slow. The fast flash powder is the best for using in explosives or detonators. It burns very rapidly, regardless of confinement or packing, with a hot white "flash", hence its name. It is fairly expensive, costing about $11.00. It is sold in magic shops and theatre supply stores.

2.06 AMMONIUM NITRATE

Ammonium nitrate is a high explosive material that is often used as a commercial "safety explosive" It is very stable, and is difficult to ignite with a match. It will only light if the glowing, red-hot part of a match is touching it. It is also difficult to detonate; (the phenomenon of detonation will be explained later) it requires a large shockwave to cause it to go high explosive. Commercially, it is sometimes mixed with a small amount of nitroglycerine to increase its sensitivity. Ammonium nitrate is used in the "Cold-Paks" or "Instant Cold", available in most drug stores. The "Cold Paks" consist of a bag of water, surrounded by a second plastic bag containing the ammonium nitrate. To get the ammonium nitrate, simply cut off the top of the outside bag, remove the plastic bag of water, and save the ammonium nitrate in a well sealed, airtight container, since it is rather hydroscopic, i.e. it tends to absorb water from the air. It is also the main ingredient in many fertilizers.

2.1 ACQUIRING CHEMICALS

The first section deals with getting chemicals legally. This section deals with "procuring" them. The best place to steal chemicals is a college. Many state schools have all of their chemicals out on the shelves in the labs, and more in their chemical stockrooms. Evening is the best time to enter lab buildings, as there are the least number of people in the buildings, and most of the labs will still be unlocked. One simply takes a bookbag, wears a dress shirt and jeans, and tries to resemble a college freshman. If anyone asks what such a person is doing, the thief can simply say that he is looking for the polymer chemistry lab, or some other chemistry-related department other than the one they are in. One can usually find out where the various labs and departments in a building are by calling the university. There are, of course other techniques for getting into labs after hours, such as placing a piece of cardboard in the latch of an unused door, such as a back exit. Then, all one needs to do is come back at a later hour. Also, before this is done, terrorists check for security systems. If one just walks into a lab, even if there is someone there, and walks out the back exit, and slip the cardboard in the latch before the door closes, the person in the lab will never know what happened. It is also a good idea to observe the building that one plans to rob at the time that one plans to rob it several days before the actual theft is done. This is advisable since the would-be thief should know when and if the campus security makes patrols through buildings. Of course, if none of these methods are successful, there is always section 2.11, but as a rule, college campus security is pretty poor, and nobody suspects another person in the building of doing anything wrong, even if they are there at an odd hour.

2.11 TECHNIQUES FOR PICKING LOCKS

If it becomes necessary to pick a lock to enter a lab, the world's most effective lockpick is dynamite, followed by a sledgehammer. There are unfortunately, problems with noise and excess structural damage with these methods. The next best thing, however, is a set of army issue lockpicks. These, unfortunately, are difficult to acquire. If the door to a lab is locked, but the deadbolt is not engaged, then there are other possibilities. The rule here is: if one can see the latch, one can open the door. There are several devices which facilitate freeing the latch from its hole in the wall. Dental tools, stiff wire (20 gauge), specially bent aluminum from cans, thin pocket- knives, and credit cards are the tools of the trade. The way that all these tools and devices are uses is similar: pull, push, or otherwise move the latch out of its hole in the wall, and pull the door open. This is done by sliding whatever tool that you are using behind the latch, and pulling the latch out from the wall. To make an aluminum-can lockpick, terrorists can use an aluminum can and carefully cut off the can top and bottom. Cut off the cans' ragged ends. Then, cut the open-ended cylinder so that it can be flattened out into a single long rectangle. This should then be cut into inch wide strips. Fold the strips in 1/4 inch increments (1). One will have a long quadruple-thick 1/4 inch wide strip of aluminum. This should be folded into an L-shape, a J-shape, or a U-shape. This is done by folding. The pieces would look like this:

(1)

```
        ____________________________________________________   v
1/4   |__________________________________________________|   |
1/4   |__________________________________________________|   | 1
inch
1/4   |__________________________________________________|   |
1/4   |__________________________________________________|   |
                                 ^
```

Fold along lines to make a single quadruple-thick piece of aluminum. This should then be folded to produce an L,J,or U shaped device that looks like this:

```
  _____________________________________
 / ___________________________________|
| |
| |        L-shaped
| |
| |
|_|


  _________________________
 / _______________________|
| |
| |    J-shaped
| |
| |_______
 \_______|
   ______________________
  / ____________________|
 | |
 | |
 | |    U-shaped
 | |
 | |_____________________
  \_____________________|
```

All of these devices should be used to hook the latch of a door and pull the latch out of its hole. The folds in the lockpicks will be between the door and the wall, and so the device will not unfold, if it is made properly.

2.2 LIST OF USEFUL HOUSEHOLD CHEMICALS AND THEIR AVAILABILITY

Anyone can get many chemicals from hardware stores, supermarkets, and drug stores to get the materials to make explosives or other dangerous compounds. A would-be terrorist would merely need a station wagon and some money to acquire many of the chemicals named here.

Chemical	Used In	Available at
alcohol, ethyl *	alcoholic beverages solvents (95% min. for both)	liquor stores hardware stores
ammonia +	CLEAR household ammonia	supermarkets/7-eleven
ammonium nitrate	instant-cold paks, fertilizers	drug stores, medical supply stores
nitrous oxide	pressurizing whip cream	party supply stores
magnesium	firestarters	surplus/camping stores
lecithin	vitamins	pharmacies/drug stores
mineral oil	cooking, laxative	supermarket/drug stores
mercury @	mercury thermometers	supermarkets/hardware stores
sulfuric acid	uncharged car batteries	automotive stores
glycerine	?	pharmacies/drug stores

sulfur	gardening	gardening/hardware store
charcoal	charcoal grills	supermarkets/gardening stores
sodium nitrate	fertilizer	gardening store
cellulose (cotton)	first aid	drug/medical supply stores
strontium nitrate	road flares	surplus/auto stores,
fuel oil	kerosene stoves	surplus/camping stores,
bottled gas	propane stoves	surplus/camping stores,
potassium permanganate	water purification	purification plants
hexamine or methenamine	hexamine stoves (camping)	surplus/camping stores
nitric acid ^	cleaning printing plates	printing shops photography stores
iodine &	first aid	drug stores
sodium perchlorate	solidox pellets for cutting torches	hardware stores

notes: * ethyl alcohol is mixed with methyl alcohol when it is used as a solvent. Methyl alcohol is very poisonous. Solvent alcohol must be at least 95% ethyl alcohol if it is used to make mercury fulminate. Methyl alcohol may prevent mercury fulminate from forming.

+ Ammonia, when bought in stores comes in a variety of forms. The pine and cloudy ammonias should not be bought; only the clear ammonia should be used to make ammonium triiodide crystals.

@ Mercury thermometers are becoming a rarity, unfortunately. They may be hard to find in most stores. Mercury is also used in mercury switches, which are available at electronics stores. Mercury is a hazardous substance, and should be kept in the thermometer or mercury switch until used. It gives off mercury vapors which will cause brain damage if inhaled. For this reason, it is a good idea not to spill mercury, and to always use it outdoors. Also, do not get it in an open cut; rubber gloves will help prevent this.

^ Nitric acid is very difficult to find nowadays. It is usually stolen by bomb makers, or made by the process described in a later section. A desired concentration for making explosives about 70%.

& The iodine sold in drug stores is usually not the pure crystaline form that is desired for producing ammonium triiodide crystals. To obtain the pure form, it must usually be acquired by a doctor's prescription, but this can be expensive. Once again, theft is the means that terrorists result to.

2.3 PREPARATION OF CHEMICALS

2.31 NITRIC ACID

There are several ways to make this most essential of all acids for explosives. One method by which it could be made will be presented. Once again, be reminded that these methods SHOULD NOT BE CARRIED OUT!!

Materials:
----
sodium nitrate or
potassium nitrate

distilled water

concentrated
sulfuric acid

Equipment:
----
adjustable heat source

retort

ice bath

stirring rod

collecting flask with stopper

1) Pour 32 milliliters of concentrated sulfuric acid into the retort.

2) Carefully weigh out 58 grams of sodium nitrate, or 68 grams of potassium nitrate. and add this to the acid slowly. If it all does not dissolve, carefully stir the solution with a glass rod until it does.

3) Place the open end of the retort into the collecting flask, and place the collecting flask in the ice bath.

4) Begin heating the retort, using low heat. Continue heating until liquid begins to come out of the end of the retort. The liquid that forms is nitric acid. Heat until the precipitate in the bottom of the retort is almost dry, or until no more nitric acid is forming. CAUTION: If the acid is headed too strongly, the nitric acid will decompose as soon as it is formed. This can result in the production of highly flammable and toxic gasses that may explode. It is a good idea to set the above apparatus up, and then get away from it.

Potassium nitrate could also be obtained from store-bought black powder, simply by dissolving black powder in boiling water and filtering out the sulfur and charcoal. To obtain 68 g of potassium nitrate, it would be necessary to dissolve about 90 g of black powder in about one litre of boiling water. Filter the dissolved solution through filter paper in a funnel into a jar until the liquid that pours through is clear. The charcoal and sulfur in black powder are insoluble in water, and so when the solution of water is allowed to evaporate, potassium nitrate will be left in the jar.

2.32 SULFURIC ACID

Sulfuric acid is far too difficult to make outside of a laboratory or industrial plant. However, it is readily available in an uncharged car battery. A person wishing to make sulfuric acid would simply remove the top of a car battery and pour the acid into a glass container. There would probably be pieces of lead from the battery in the acid which would have to be removed, either by boiling or filtration. The concentration of the sulfuric acid can also be increased by boiling it; very pure sulfuric acid pours slightly faster than clean motor oil.

2.33 AMMONIUM NITRATE

Ammonium nitrate is a very powerful but insensitive high-order explosive. It could be made very easily by pouring nitric acid into a large flask in an ice bath. Then, by simply pouring household ammonia into the flask and running away, ammonium nitrate would be formed. After the materials have stopped reacting, one would simply have to leave the solution in a warm place until all of the water and any unneutralized ammonia or acid have evaporated. There would be a fine powder formed, which would be ammonium nitrate. It must be kept in an airtight container, because of its tendency to pick up water from the air. The crystals formed in the above process would have to be heated VERY gently to drive off the remaining water.

3.0 EXPLOSIVE RECIPES

Once again, persons reading this material MUST NEVER ATTEMPT TO PRODUCE ANY OF THE EXPLOSIVES DESCRIBED HEREIN. IT IS ILLEGAL AND EXTREMELY DANGEROUS TO ATTEMPT TO DO SO. LOSS OF LIFE AND/OR LIMB COULD EASILY OCCUR AS A RESULT OF ATTEMPTING TO PRODUCE EXPLOSIVE MATERIALS.

These recipes are theoretically correct, meaning that an individual could conceivably produce the materials described. The methods here are usually scaled-down industrial procedures.

3.01 EXPLOSIVE THEORY

An explosive is any material that, when ignited by heat or shock, undergoes rapid decomposition or oxidation. This process releases energy that is stored in the material in the form of heat and light, or by breaking down into gaseous compounds that occupy a much larger volume that the original piece of material. Because this expansion is very rapid, large volumes of air are displaced by the expanding gasses. This expansion occurs at a speed greater than the speed of sound, and so a sonic boom occurs. This explains the mechanics behind an explosion. Explosives occur in several forms: high-order explosives which detonate, low order explosives, which burn, and primers, which may do both.

High order explosives detonate. A detonation occurs only in a high order explosive. Detonations are usually incurred by a shockwave that passes through a block of the high explosive material. The shockwave breaks apart the molecular bonds between the atoms of the substance, at a rate approximately equal to the speed of sound traveling through that material. In a high explosive, the fuel and oxodizer are chemically bonded, and the shockwave breaks apart these bonds, and re-combines the two materials to produce mostly gasses. T.N.T., ammonium nitrate, and R.D.X. are examples of high order explosives.

Low order explosives do not detonate; they burn, or undergo oxidation. when heated, the fuel(s) and oxodizer(s) combine to produce heat, light, and gaseous products. Some low order materials burn at about the same speed under pressure as they do in the open, such as blackpowder. Others, such as gunpowder, which is correctly called nitrocellulose, burn much faster and hotter when they are in a confined space, such as the barrel of a firearm; they usually burn much slower than blackpowder when they are ignited in unpressurized conditions. Black powder, nitrocellulose, and flash powder are good examples of low order explosives.

Primers are peculiarities to the explosive field. Some of them, such as mercury filminate, will function as a low or high order explosive. They are usually more sensitive to friction, heat, or shock, than the high or low explosives. Most primers perform like a high order explosive, except that they are much more sensitive. Still others merely burn, but when they are confined, they burn at a great rate and with a large expansion of gasses and a shockwave. Primers are usually used in a small amount to initiate, or cause to decompose, a high order explosive, as in an artillery shell. But, they are also frequently used to ignite a low order explosive; the gunpowder in a bullet is ignited by the detonation of its primer.

3.1 IMPACT EXPLOSIVES

Impact explosives are often used as primers. Of the ones discussed here, only mercury fulminate and nitroglycerine are real explosives; Ammonium triiodide crystals decompose upon impact, but they release little heat and no light. Impact explosives are always treated with the greatest care, and even the stupidest anarchist never stores them near any high or low explosives.

3.11 AMMONIUM TRIIODIDE CRYSTALS

Ammonium triiodide crystals are foul-smelling purple colored crystals that decompose under the slightest amount of heat, friction, or shock, if they are made with the purest ammonia (ammonium hydroxide) and iodine. Such crystals are said to detonate when a fly lands on them, or when an ant walks across them. Household ammonia, however, has enough impurities, such as soaps and abrasive agents, so that the crystals will detonate when thrown,crushed, or heated. Upon detonation, a loud report is heard, and a cloud of purple iodine gas appears about the detonation site. Whatever the unfortunate surface that the crystal was detonated upon will usually be ruined, as some of the iodine in the crystal is thrown about in a solid form, and iodine is corrosive. It leaves nasty, ugly, permanent brownish-purple stains on whatever it contacts. Iodine gas is also bad news, since it can damage lungs, and it settles to the ground and stains things there also. Touching iodine leaves brown stains on the skin that last for about a week, unless they are immediately and vigorously washed off. While such a compound would have little use to a serious terrorist, a vandal could utilize them in damaging property. Or, a terrorist could throw several of them into a crowd as a distraction, an action which would possibly injure a few people, but frighten almost anyone, since a small crystal that not be seen when thrown produces a rather loud explosion. Ammonium triiodide crystals could be produced in the following manner:

Materials	Equipment
iodine crystals	funnel and filter paper
	paper towels
clear ammonia (ammonium hydroxide, for the suicidal)	two throw-away glass jars

1) Place about two teaspoons of iodine into one of the glass jars. The jars must both be throw away because they will never be clean again.

2) Add enough ammonia to completely cover the iodine.

3) Place the funnel into the other jar, and put the filter paper in the funnel.
The technique for putting filter paper in a funnel is taught in every basic chemistry lab class: fold the circular paper in half, so that a semi-circle is formed. Then, fold it in half again to form a triangle with one curved side. Pull one thickness of paper out to form a cone, and place the cone into the funnel.

4) After allowing the iodine to soak in the ammonia for a while, pour the solution into the paper in the funnel through the filter paper.

5) While the solution is being filtered, put more ammonia into the first jar to wash any remaining crystals into the funnel as soon as it drains.

6) Collect all the purplish crystals without touching the brown filter paper, and place them on the paper towels to dry for about an hour. Make sure that they are not too close to any lights or other sources of heat, as they could well detonate. While they are still wet, divide

the wet material into about eight chunks.

7) After they dry, gently place the crystals onto a one square inch piece of duct tape. Cover it with a similar piece, and gently press the duct tape together around the crystal, making sure not to press the crystal itself. Finally, cut away most of the excess duct tape with a pair of scissors, and store the crystals in a cool dry safe place. They have a shelf life of about a week, and they should be stored in individual containers that can be thrown away, since they have a tendency to slowly decompose, a process which gives off iodine vapors, which will stain whatever they settle on. One possible way to increase their shelf life is to store them in airtight containers. To use them, simply throw them against any surface or place them where they will be stepped on or crushed.

3.12 MERCURY FULMINATE

Mercury fulminate is perhaps one of the oldest known initiating compounds. It can be detonated by either heat or shock, which would make it of infinite value to a terrorist. Even the action of dropping a crystal of the fulminate causes it to explode. A person making this material would probably use the following procedure:

MATERIALS	EQUIPMENT
mercury (5 g)	glass stirring rod
concentrated nitric acid (35 ml)	100 ml beaker (2)
ethyl alcohol (30 ml)	adjustable heat source
distilled water	blue litmus paper
funnel and filter paper	

1) In one beaker, mix 5 g of mercury with 35 ml of concentrated nitric acid, using the glass rod.

2) Slowly heat the mixture until the mercury is dissolved, which is when the solution turns green and boils.

3) Place 30 ml of ethyl alcohol into the second beaker, and slowly and carefully add all of the contents of the first beaker to it. Red and/or brown fumes should appear. These fumes are toxic and flammable.

4) After thirty to forty minutes, the fumes should turn white, indicating that the reaction is near completion. After ten more minutes, add 30 ml of the distilled water to the solution.

5) Carefully filter out the crystals of mercury fulminate from the liquid solution. Dispose of the solution in a safe place, as it is corrosive and

toxic.

6) Wash the crystals several times in distilled water to remove as much excess acid as possible. Test the crystals with the litmus paper until they are neutral. This will be when the litmus paper stays blue when it touches the wet crystals

7) Allow the crystals to dry, and store them in a safe place, far away from any explosive or flammable material.

This procedure can also be done by volume, if the available mercury cannot be weighed. Simply use 10 volumes of nitric acid and 10 volumes of ethanol to every one volume of mercury.

3.13 NITROGLYCERINE

Nitroglycerine is one of the most sensitive explosives, if it is not the most sensitive. Although it is possible to make it safely, it is difficult. Many a young anarchist has been killed or seriously injured while trying to make the stuff. When Nobel's factories make it, many people were killed by the all-to-frequent factory explosions. Usually, as soon as it is made, it is converted into a safer substance, such as dynamite. An idiot who attempts to make nitroglycerine would use the following procedure:

MATERIAL --------	EQUIPMENT ---------
distilled water	eye-dropper
table salt	100 ml beaker
sodium bicarbonate	200-300 ml beakers (2)
concentrated nitric acid (13 ml)	ice bath container (a plastic bucket serves well)
concentrated sulfuric acid (39 ml)	centigrade thermometer
	blue litmus paper
glycerine	

1) Place 150 ml of distilled water into one of the 200-300 ml beakers.

2) In the other 200-300 ml beaker, place 150 ml of distilled water and about a spoonful of sodium bicarbonate, and stir them until the sodium bicarbonate dissolves. Do not put so much sodium bicarbonate in the water so that some remains undissolved.

3) Create an ice bath by half filling the ice bath container with ice, and adding table salt. This will cause the ice to melt, lowering the overall temperature.

3.14 PICRATES

Although the procedure for the production of picric acid, or trinitrophenol has not yet been given, its salts are described first, since they are extremely sensitive, and detonate on impact. By mixing picric acid with metal hydroxides, such as sodium or potassium hydroxide, and evaporating the water, metal picrates can be formed. Simply obtain picric acid, or produce it, and mix it with a solution of (preferably) potassium hydroxide, of a mid range molarity. (about 6-9 M) This material, potassium picrate, is impact-sensitive, and can be used as an initiator for any type of high explosive.

3.2 LOW-ORDER EXPLOSIVES

There are many low-order explosives that can be purchased in gun stores and used in explosive devices. However, it is possible that a wise wise store owner would not sell these substances to a suspicious-looking individual. Such an individual would then be forced to resort to making his own low-order explosives.

3.21 BLACK POWDER

First made by the Chinese for use in fireworks, black powder was first used in weapons and explosives in the 12th century. It is very simple to make, but it is not very powerful or safe. Only about 50% of black powder is converted to hot gasses when it is burned; the other half is mostly very fine burned particles. Black powder has one major problem: it can be ignited by static electricity. This is very bad, and it means that the material must be made with wooden or clay tools. Anyway, a misguided individual could manufacture black powder at home with the following procedure:

MATERIALS	EQUIPMENT
potassium nitrate (75 g)	clay grinding bowl and clay grinder
or	or
sodium nitrate (75 g)	wooden salad bowl and wooden spoon
sulfur (10 g)	plastic bags (3)
charcoal (15 g)	300-500 ml beaker (1)

distilled water	coffee pot or heat source

1) Place a small amount of the potassium or sodium nitrate in the grinding bowl and grind it to a very fine powder. Do this to all of the potassium or sodium nitrate, and store the ground powder in one of the plastic bags.

2) Do the same thing to the sulfur and charcoal, storing each chemical in a separate plastic bag.

3) Place all of the finely ground potassium or sodium nitrate in the beaker, and add just enough boiling water to the chemical to get it all wet.

4) Add the contents of the other plastic bags to the wet potassium or sodium nitrate, and mix them well for several minutes. Do this until there is no more visible sulfur or charcoal, or until the mixture is universally black.

5) On a warm sunny day, put the beaker outside in the direct sunlight. Sunlight is really the best way to dry black powder, since it is never too hot, but it is hot enough to evaporate the water.

6) Scrape the black powder out of the beaker, and store it in a safe container. Plastic is really the safest container, followed by paper. Never store black powder in a plastic bag, since plastic bags are prone to generate static electricity.

3.22 NITROCELLULOSE

Nitrocellulose is usually called "gunpowder" or "guncotton". It is more stable than black powder, and it produces a much greater volume of hot gas. It also burns much faster than black powder when it is in a confined space. Finally, nitrocellulose is fairly easy to make, as outlined by the following procedure:

MATERIALS ---------	EQUIPMENT ---------
cotton (cellulose)	two (2) 200-300 ml beakers
concentrated nitric acid	funnel and filter paper
	blue litmus paper
concentrated sulfuric acid	
distilled water	

1) Pour 10 cc of concentrated sulfuric acid into the beaker. Add to this 10 cc of concentrated nitric acid.

2) Immediately add 0.5 gm of cotton, and allow it to soak for exactly 3 minutes.

3) Remove the nitrocotton, and transfer it to a beaker of distilled water to wash it in.

4) Allow the material to dry, and then re-wash it.

5) After the cotton is neutral when tested with litmus paper, it is ready to be dried and stored.

3.23 FUEL-OXODIZER MIXTURES

There are nearly an infinite number of fuel-oxodizer mixtures that can be produced by a misguided individual in his own home. Some are very effective and dangerous, while others are safer and less effective. A list of working fuel-oxodizer mixtures will be presented, but the exact measurements of each compound are debatable for maximum effectiveness. A rough estimate will be given of the percentages of each fuel and oxodizer:

oxodizer, % by weight	fuel, % by weight	speed #	notes
potassium chlorate 67%	sulfur 33%	5	friction/impact sensitive; unstable
potassium chlorate 50%	sugar 35% charcoal 15%	5	fairly slow burning; unstable
potassium chlorate 50%	sulfur 25% magnesium or aluminum dust 25%	8	extremely unstable!
potassium chlorate 67%	magnesium or aluminum dust 33%	8	unstable
sodium nitrate 65%	magnesium dust 30% sulfur 5%	?	unpredictable burn rate
potassium permanganate 60% WARNING: IGNITES SPONTANEOUSLY WITH GLYCERINE!!!	glycerine 40%	4	delay before ignition depends upon grain size
potassium permanganate 67%	sulfur 33%	5	unstable
potassium permangenate 60%	sulfur 20% magnesium or aluminum dust 20%	5	unstable
potassium permanganate 50%	sugar 50%	3	?

potassium nitrate 75%	charcoal 15% sulfur 10%	7	this is black powder!
potassium nitrate 60%	powdered iron or magnesium 40%	1	burns very hot

oxidizer, % by weight	fuel, % by weight	speed #	notes
potassium chlorate 75%	phosphorus sesquisulfide 25%	8	used to make strike-anywhere matches
ammonium perchlorate 70%	aluminum dust 30% and small amount of iron oxide	6	solid fuel for space shuttle
potassium perchlorate 67% (sodium perchlorate)	magnesium or aluminum dust 33%	10	flash powder
potassium perchlorate 60% (sodium perchlorate)	magnesium or aluminum dust 20% sulfur 20%	8	alternate flash powder
barium nitrate 30% potassium perchlorate 30%	aluminum dust 30%	9	alternate flash powder
barium peroxide 90%	magnesium dust 5% aluminum dust 5%	10	alternate flash powder
potassium perchlorate 50%	sulfur 25% magnesium or aluminum dust 25%	8	slightly unstable
potassium chlorate 67% calcium carbonate 3%	red phosphorus 27% sulfur 3%	7	very unstable impact sensitive
potassium permanganate 50%	powdered sugar 25% aluminum or magnesium dust 25%	7	unstable; ignites if it gets wet!
potassium chlorate 75%	charcoal dust 15% sulfur 10%	6	unstable

NOTE: Mixtures that uses substitutions of sodium perchlorate for potassium perchlorate become moisture-absorbent and less stable.

The higher the speed number, the faster the fuel-oxodizer mixture burns AFTER ignition. Also, as a rule, the finer the powder, the faster the rate of burning.

As one can easily see, there is a wide variety of fuel-oxodizer mixtures that can be made at home. By altering the amounts of fuel and oxodizer(s), different burn rates can be achieved, but this also can change the sensitivity of the mixture.

3.24 PERCHLORATES

As a rule, any oxidizable material that is treated with perchloric acid will become a low order explosive. Metals, however, such as potassium or sodium, become excellent bases for flash-type powders. Some materials that can be perchlorated are cotton, paper, and sawdust. To produce potassium or sodium perchlorate, simply acquire the hydroxide of that metal, e.g. sodium or potassium hydroxide. It is a good idea to test the material to be perchlorated with a very small amount of acid, since some of the materials tend to react explosively when contacted by the acid. Solutions of sodium or potassium hydroxide are ideal.

3.3 HIGH-ORDER EXPLOSIVES

High order explosives can be made in the home without too much difficulty. The main problem is acquiring the nitric acid to produce the high explosive. Most high explosives detonate because their molecular structure is made up of some fuel and usually three or more NO2 (nitrogen dioxide) molecules. T.N.T., or Tri-Nitro-Toluene is an excellent example of such a material. When a shock wave passes through an molecule of T.N.T., the nitrogen dioxide bond is broken, and the oxygen combines with the fuel, all in a matter of microseconds. This accounts for the great power of nitrogen-based explosives. Remembering that these procedures are NEVER TO BE CARRIED OUT, several methods of manufacturing high-order explosives in the home are listed.

3.31 R.D.X.

R.D.X., also called cyclonite, or composition C-1 (when mixed with plasticisers) is one of the most valuable of all military explosives. This is because it has more than 150% of the power of T.N.T., and is much easier to detonate. It should not be used alone, since it can be set off by a not-too severe shock. It is less sensitive than mercury fulminate, or nitroglycerine, but it is still too sensitive to be used alone. R.D.X. can be made by the surprisingly simple method outlined hereafter. It is much easier to make in the home than all other high explosives, with the possible exception of ammonium nitrate.

MATERIALS	EQUIPMENT
---------	---------
hexamine	500 ml beaker
or	
methenamine	glass stirring rod
fuel tablets (50 g)	
	funnel and filter paper
concentrated	
nitric acid (550 ml)	ice bath container
	(plastic bucket)
distilled water	
	centigrade thermometer
table salt	
	blue litmus paper
ice	
ammonium nitrate	

1) Place the beaker in the ice bath, (see section 3.13, steps 3-4) and carefully pour 550 ml of concentrated nitric acid into the beaker.

2) When the acid has cooled to below 20 degrees centigrade, add small amounts of the crushed fuel tablets to the beaker. The temperature will rise, and it must be kept below 30 degrees centigrade, or dire consequences could result. Stir the mixture.

3) Drop the temperature below zero degrees centigrade, either by adding more ice and salt to the old ice bath, or by creating a new ice bath. Or, ammonium nitrate could be added to the old ice bath, since it becomes cold when it is put in water. Continue stirring the mixture, keeping the temperature below zero degrees centigrade for at least twenty minutes

4) Pour the mixture into a litre of crushed ice. Shake and stir the mixture, and allow it to melt. Once it has melted, filter out the crystals, and dispose of the corrosive liquid.

5) Place the crystals into one half a litre of boiling distilled water. Filter the crystals, and test them with the blue litmus paper. Repeat steps 4 and 5 until the litmus paper remains blue. This will make the crystals more stable and safe.

6) Store the crystals wet until ready for use. Allow them to dry completely using them. R.D.X. is not stable enough to use alone as an explosive.

7) Composition C-1 can be made by mixing 88.3% R.D.X. (by weight) with 11.1% mineral oil, and 0.6% lecithin. Kneed these material together in a plastic bag. This is a good way to desensitize the explosive.

8) H.M.X. is a mixture of T.N.T. and R.D.X.; the ratio is 50/50, by weight. it is not as sensitive, and is almost as powerful as straight R.D.X.

9) By adding ammonium nitrate to the crystals of R.D.X. after step 5, it

should be possible to desensitize the R.D.X. and increase its power, since ammonium nitrate is very insensitive and powerful. Soduim or potassium nitrate could also be added; a small quantity is sufficient to stabilize the R.D.X.

10) R.D.X. detonates at a rate of 8550 meters/second when it is compressed to a density of 1.55 g/cubic cm.

3.32 AMMONIUM NITRATE

Ammonium nitrate could be made by a terrorist according to the haphazard method in section 2.33, or it could be stolen from a construction site, since it is usually used in blasting, because it is very stable and insensitive to shock and heat. A terrorist could also buy several Instant Cold-Paks from a drug store or medical supply store. The major disadvantage with ammonium nitrate, from a terrorist's point of view, would be detonating it. A rather powerful priming charge must be used, and usually with a booster charge. The diagram below will explain.

```
      _____________________________________________
      |    |                 |
 _________|    |                 |
   |    | T.N.T.|   ammonium nitrate    |
   |primer |booster|                |
   |_______|    |                |
      |    |                 |
      |_______|__________________________________|
```

The primer explodes, detonating the T.N.T., which detonates, sending a tremendous shockwave through the ammonium nitrate, detonating it.

3.33 ANFOS

ANFO is an acronym for Ammonium Nitrate - Fuel Oil Solution. An ANFO solves the only other major problem with ammonium nitrate: its tendency to pick up water vapor from the air. This results in the explosive failing to detonate when such an attempt is made. This is rectified by mixing 94% (by weight) ammonium nitrate with 6% fuel oil, or kerosene. The kerosene keeps the ammonium nitrate from absorbing moisture from the air. An ANFO also requires a large shockwave to set it off.

3.34 T.N.T.

T.N.T., or Tri-Nitro-Toluene, is perhaps the second oldest known high explosive. Dynamite, of course, was the first. It is certainly the best known high explosive, since it has been popularized by early morning cartoons. It is the standard for comparing other explosives to, since it is the most well known. In industry, a T.N.T. is made by a three step nitration process that is designed to conserve the nitric and sulfuric acids which are used to make the product. A terrorist, however, would probably opt for the less economical one step method. The one step process is performed by treating toluene with very strong (fuming) sulfuric acid. Then, the sulfated toluene is treated with very strong (fuming) nitric acid in an ice bath. Cold water is added the solution, and it is filtered.

3.35 POTASSIUM CHLORATE

Potassium chlorate itself cannot be made in the home, but it can be obtained from labs. If potassium chlorate is mixed with a small amount of vaseline, or other petroleum jelly, and a shockwave is passed through it, the material will detonate with slightly more power than black powder. It must, however, be confined to detonate it in this manner. The procedure for making such an explosive is outlined below:

MATERIALS ---------	EQUIPMENT ---------
potassium chlorate (9 parts, by volume)	zip-lock plastic bag
petroleum jelly (vaseline) (1 part, by volume)	clay grinding bowl or wooden bowl and wooden spoon

1) Grind the potassium chlorate in the grinding bowl carefully and slowly, until the potassium chlorate is a very fine powder. The finer that it is powdered, the faster (better) it will detonate.

2) Place the powder into the plastic bag. Put the petroleum jelly into the plastic bag, getting as little on the sides of the bag as possible, i.e. put the vaseline on the potassium chlorate powder.

3) Close the bag, and kneed the materials together until none of the potassium chlorate is dry powder that does not stick to the main glob. If necessary, add a bit more petroleum jelly to the bag.

4) The material must me used within 24 hours, or the mixture will react to greatly reduce the effectiveness of the explosive. This reaction, however, is harmless, and releases no heat or dangerous products.

3.36 DYNAMITE

The name dynamite comes from the Greek word "dynamis", meaning power. Dynamite was invented by Nobel shortly after he made nitroglycerine. It was made because nitroglycerine was so dangerously sensitive to shock. A misguided individual with some sanity would, after making nitroglycerine (an insane act) would immediately convert it to dynamite. This can be done by adding various materials to the nitroglycerine, such as sawdust. The sawdust holds a large weight of nitroglycerine per volume. Other materials, such as ammonium nitrate could be added, and they would tend to desensitize the explosive, and increase the power. But even these nitroglycerine compounds are not really safe.

3.37 NITROSTARCH EXPLOSIVES

Nitrostarch explosives are simple to make, and are fairly powerful. All that need be done is treat various starches with a mixture of concentrated nitric and sulfuric acids. 10 ml of concentrated sulfuric acid is added to 10 ml of concentrated nitric acid. To this mixture is added 0.5 grams of starch. Cold water is added, and the apparently unchanged nitrostarch is filtered out. Nitrostarch explosives are of slightly lower power than T.N.T., but they are more readily detonated.

3.38 PICRIC ACID

Picric acid, also known as Tri-Nitro-Phenol, or T.N.P., is a military explosive that is most often used as a booster charge to set off another less sensitive explosive, such as T.N.T. It another explosive that is fairly simple to make, assuming that one can acquire the concentrated sulfuric and nitric acids. Its procedure for manufacture is given in many college chemistry lab manuals, and is easy to follow. The main problem with picric acid is its tendency to form dangerously sensitive and unstable picrate salts, such as potassium picrate. For this reason, it is usually made into a safer form, such as ammonium picrate, also called explosive D. A social deviant would probably use a formula similar to the one presented here to make picric acid.

MATERIALS	EQUIPMENT
phenol (9.5 g)	500 ml flask
concentrated sulfuric acid (12.5 ml)	adjustable heat source
concentrated nitric acid (38 ml)	1000 ml beaker or other container suitable for boiling in
distilled water	filter paper and funnel
	glass stirring rod

1) Place 9.5 grams of phenol into the 500 ml flask, and carefully add 12.5 ml of concentrated sulfuric acid and stir the mixture.

2) Put 400 ml of tap water into the 1000 ml beaker or boiling container and bring the water to a gentle boil.

3) After warming the 500 ml flask under hot tap water, place it in the boiling water, and continue to stir the mixture of phenol and acid for about thirty minutes. After thirty minutes, take the flask out, and allow it to cool for about five minutes.

4) Pour out the boiling water used above, and after allowing the container to cool, use it to create an ice bath, similar to the one used in section 3.13, steps 3-4. Place the 500 ml flask with the mixed acid an phenol in the ice bath. Add 38 ml of concentrated nitric acid in small amounts, stirring the mixture constantly. A vigorous but "harmless" reaction should occur. When the mixture stops reacting vigorously, take the flask out of the ice bath.

5) Warm the ice bath container, if it is glass, and then begin boiling more tap water. Place the flask containing the mixture in the boiling water, and heat it in the boiling water for 1.5 to 2 hours.

6) Add 100 ml of cold distilled water to the solution, and chill it in an ice bath until it is cold.

7) Filter out the yellowish-white picric acid crystals by pouring the solution through the filter paper in the funnel. Collect the liquid and dispose of it in a safe place, since it is corrosive.

8) Wash out the 500 ml flask with distilled water, and put the contents of the filter paper in the flask. Add 300 ml of water, and shake vigorously.

9) Re-filter the crystals, and allow them to dry.

10) Store the crystals in a safe place in a glass container, since they will react with metal containers to produce picrates that could explode spontaneously.

3.39 AMMONIUM PICRATE

Ammonium picrate, also called Explosive D, is another safety explosive. It requires a substantial shock to cause it to detonate, slightly less than that required to detonate ammonium nitrate. It is much safer than picric acid, since it has little tendency to form hazardous unstable salts when placed in metal containers. It is simple to make from picric acid and clear household ammonia. All that need be done is put the picric acid crystals into a glass container and dissolve them in a great quantity of hot water. Add clear household ammonia in excess, and allow the excess ammonia to evaporate. The powder remaining should be ammonium picrate.

3.40 NITROGEN TRICHLORIDE

Nitrogen trichloride, also known as chloride of azode, is an oily yellow liquid. It explodes violently when it is heated above 60 degrees celsius, or when it comes in contact with an open flame or spark. It is fairly simple to produce.

3.41 LEAD AZIDE

Lead Azide is a material that is often used as a booster charge for other explosive, but it does well enough on its own as a fairly sensitive explosive. It does not detonate too easily by percussion or impact, but it is easily detonated by heat from an igniter wire, or a blasting cap. It is simple to produce, assuming that the necessary chemicals can be procured.

3.5 OTHER "EXPLOSIVES"

The remaining section covers the other types of materials that can be used to destroy property by fire. Although none of the materials presented here are explosives, they still produce explosive-style results.

3.51 THERMIT

Thermit is a fuel-oxodizer mixture that is used to generate tremendous amounts of heat. It was not presented in section 3.23 because it does not react nearly as readily. It is a mixture of iron oxide and aluminum, both finely powdered. When it is ignited, the aluminum burns, and extracts the oxygen from the iron oxide. This is really two very exothermic reactions that produce a combined temperature of about 2200 degrees C. This is half the heat produced by an atomic weapon. It is difficult to ignite, however, but when it is ignited, it is one of the most effective firestarters around.

MATERIALS
----

powdered aluminum (10 g)

powdered iron oxide (10 g)

1) There is no special procedure or equipment required to make thermit. Simply mix the two powders together, and try to make the mixture as homogenous as possible. The ratio of iron oxide to aluminum is 50% / 50% by weight, and be made in greater or lesser amounts.

2) Ignition of thermite can be accomplished by adding a small amount of potassium chlorate to the thermit, and pouring a few drops of sulfuric acid on it. This method and others will be discussed later in section 4.33. The other method of igniting thermit is with a magnesium strip. Finally, by using common sparkler-type fireworks placed in the thermit, the mixture can be ignited.

3.52 MOLOTOV COCKTAILS

First used by Russians against German tanks, the Molotov cocktail is now exclusively used by terrorists worldwide. They are extremely simple to make, and can produce devastating results. By taking any highly flammable material, such as gasoline, diesel fuel, kerosene, ethyl or methyl alcohol, lighter fluid, turpentine, or any mixture of the above, and putting it into a large glass bottle, anyone can make an effective firebomb. After putting the flammable liquid in the bottle, simply put a piece of cloth that is soaked in the liquid in the top of the bottle so that it fits tightly. Then, wrap some of the cloth around the neck and tie it, but be sure to leave a few inches of lose cloth to light. Light the exposed cloth, and throw the bottle. If the burning cloth does not go out, and if the bottle breaks on impact, the contents of the bottle will spatter over a large area near the site of impact, and burst into flame. Flammable mixtures such as kerosene and motor oil should be mixed with a more volatile and flammable liquid, such as gasoline, to insure ignition. A mixture such as tar or grease and gasoline will stick to the surface that it strikes, and burn hotter, and be more difficult to extinguish. A mixture such as this must be shaken well before it is lit and thrown

3.53 CHEMICAL FIRE BOTTLE

The chemical fire bottle is really an advanced molotov cocktail. Rather than using the burning cloth to ignite the flammable liquid, which has at best a fair chance of igniting the liquid, the chemical fire bottle utilizes the very hot and violent reaction between sulfuric acid and potassium chlorate. When the container breaks, the sulfuric acid in the mixture of gasoline sprays onto the paper soaked in potassium chlorate and sugar. The paper, when struck by the acid, instantly bursts into a white flame, igniting the gasoline. The chance of failure to ignite the gasoline is less than 2%, and can be reduced to 0%, if there is enough potassium chlorate and sugar to spare.

MATERIALS	EQUIPMENT
---------	---------
potassium chlorate (2 teaspoons)	glass bottle (12 oz.)
sugar (2 teaspoons)	cap for bottle, with plastic inside
concentrated sulfuric acid (4 oz.)	cooking pan with raised edges
gasoline (8 oz.)	paper towels
	glass or plastic cup and spoon

1) Test the cap of the bottle with a few drops of sulfuric acid to make sure that the acid will not eat away the bottle cap during storage. If the acid eats through it in 24 hours, a new top must be found and tested, until a cap that the acid does not eat through is found. A glass top is excellent.

2) Carefully pour 8 oz. of gasoline into the glass bottle.

3) Carefully pour 4 oz. of concentrated sulfuric acid into the glass bottle. Wipe up any spills of acid on the sides of the bottle, and screw the cap on the bottle. Wash the bottle's outside with plenty of water. Set it aside to dry.

4) Put about two teaspoons of potassium chlorate and about two teaspoons of sugar into the glass or plastic cup. Add about 1/2 cup of boiling water, or enough to dissolve all of the potassium chlorate and sugar.

5) Place a sheet of paper towel in the cooking pan with raised edges. Fold the paper towel in half, and pour the solution of dissolved potassium chlorate and sugar on it until it is thoroughly wet. Allow the towel to

dry.

6) When it is dry, put some glue on the outside of the glass bottle containing the gasoline and sulfuric acid mixture. Wrap the paper towel around the bottle, making sure that it sticks to it in all places. Store the bottle in a place where it will not be broken or tipped over.

7) When finished, the solution in the bottle should appear as two distinct liquids, a dark brownish-red solution on the bottom, and a clear solution on top. The two solutions will not mix. To use the chemical fire bottle, simply throw it at any hard surface.

8) NEVER OPEN THE BOTTLE, SINCE SOME SULFURIC ACID MIGHT BE ON THE CAP, WHICH COULD TRICKLE DOWN THE SIDE OF THE BOTTLE AND IGNITE THE POTASSIUM CHLORATE, CAUSING A FIRE AND/OR EXPLOSION.

9) To test the device, tear a small piece of the paper towel off the bottle, and put a few drops of sulfuric acid on it. The paper towel should immediately burst into a white flame.

3.54 BOTTLED GAS EXPLOSIVES

Bottled gas, such as butane for refilling lighters, propane for propane stoves or for bunsen burners, can be used to produce a powerful explosion. To make such a device, all that a simple-minded anarchist would have to do would be to take his container of bottled gas and place it above a can of Sterno or other gelatinized fuel, and light the fuel and run. Depending on the fuel used, and on the thickness of the fuel container, the liquid gas will boil and expand to the point of bursting the container in about five minutes. In theory, the gas would immediately be ignited by the burning gelatinized fuel, producing a large fireball and explosion. Unfortunately, the bursting of the bottled gas container often puts out the fuel, thus preventing the expanding gas from igniting. By using a metal bucket half filled with gasoline, however, the chances of ignition are better, since the gasoline is less likely to be extinguished. Placing the canister of bottled gas on a bed of burning charcoal soaked in gasoline would probably be the most effective way of securing ignition of the expanding gas, since although the bursting of the gas container may blow out the flame of the gasoline, the burning charcoal should immediately re-ignite it. Nitrous oxide, hydrogen, propane, acetylene, or any other flammable gas will do nicely.

4.0 USING EXPLOSIVES

Once a terrorist has made his explosives, the next logical step is to apply them. Explosives have a wide range of uses, from harassment, to vandalism, to murder. NONE OF THE IDEAS PRESENTED HERE ARE EVER TO BE CARRIED OUT, EITHER IN PART OR IN FULL! DOING SO CAN LEAD TO PROSECUTION, FINES, AND IMPRISONMENT!

The first step that a person that would use explosive would take would be to determine how big an explosive device would be needed to do whatever had to be done. Then, he would have to decide what to make his bomb with. He would also have to decide on how he wanted to detonate the device, and determine where the best placement for it would be. Then, it would be necessary to see if the device could be put where he wanted it without it being discovered or moved. Finally, he would actually have to sit down and build his explosive device. These are some of the topics covered in the next section.

4.1 SAFETY

There is no such thing as a "safe" explosive device. One can only speak in terms of relative safety, or less unsafe.

4.2 IGNITION DEVICES

There are many ways to ignite explosive devices. There is the classic "light the fuse, throw the bomb, and run" approach, and there are sensitive mercury switches, and many things in between. Generally, electrical detonation systems are safer than fuses, but there are times when fuses are more appropriate than electrical systems; it is difficult to carry an electrical detonation system into a stadium, for instance, without being caught. A device with a fuse or impact detonating fuse would be easier to hide.

4.21 FUSE IGNITION

The oldest form of explosive ignition, fuses are perhaps the favorite type of simple ignition system. By simply placing a piece of waterproof fuse in a device, one can have almost guaranteed ignition. Modern waterproof fuse is extremely reliable, burning at a rate of about 2.5 seconds to the inch. It is available as model rocketry fuse in most hobby shops, and costs about $3.00 for a nine-foot length. Fuse is a popular ignition system for pipe bombers because of its simplicity. All that need be done is light it with a match or lighter.

Of course, if the Army had fuses like this, then the grenade, which uses fuse ignition, would be very impracticle. If a grenade ignition system can be acquired, by all means, it is the most effective. But, since such things do not just float around, the next best thing is to prepare a fuse system which does not require the use of a match or lighter, but still retains its simplicity. One such method is described below:

MATERIALS
____

strike-on-cover type matches

electrical tape or duct tape

waterproof fuse

1) To determine the burn rate of a particular type of fuse, simply measure a 6 inch or longer piece of fuse and ignite it. With a stopwatch, press the start button the at the instant when the fuse lights, and stop the watch when the fuse reaches its end. Divide the time of burn by the length of fuse, and you have the burn rate of the fuse, in seconds per inch. This will be shown below:

Suppose an eight inch piece of fuse is burned, and its complete time of combustion is 20 seconds.

```
20 seconds
----------  = 2.5 seconds per inch.
8 inches
```

If a delay of 10 seconds was desired with this fuse, divide the desired time by the number of seconds per inch:

```
10 seconds
------------------- = 4 inches
2.5 seconds / inch
```

NOTE: THE LENGTH OF FUSE HERE MEANS LENGTH OF FUSE TO THE POWDER. SOME FUSE, AT LEAST AN INCH, SHOULD BE INSIDE THE DEVICE. ALWAYS A-- THIS EXTRA INCH, AND PUT THIS EXTRA INCH AN INCH INTO THE DEVICE!!!

2) After deciding how long a delay is desired before the explosive device is to go off, add about 1/2 an inch to the premeasured amount of fuse, and cut it off.

3) Carefully remove the cardboard matches from the paper match case. Do not pull off individual matches; keep all the matches attached to the cardboard base. Take one of the cardboard match sections, and leave the other one to make a second igniter.

4) Wrap the matches around the end of the fuse, with the heads of the matches touching the very end of the fuse. Tape them there securely, making sure not to put tape over the match heads. Make sure they are very secure by pulling on them at the base of the assembly. They should not be able to move.

5) Wrap the cover of the matches around the matches attached to the fuse, making sure that the striker paper is below the match heads and the striker faces the match heads. Tape the paper so that is fairly tight around the matches. Do not tape the cover of the striker to the fuse or to the matches. Leave enough of the match book to pull on for ignition.

```
 ______________________
 \                /
  \              /  ------ match book cover
   \            /
    |   M|f|M ---|------- match head
```

```
|    A|u|A    |
|    T|s|T    |
|    C|e|C    |
|tapeH|.|Htape|
|     |f|     |
|#####|u|#####|-------- striking paper
|#####|s|#####|
\     |e|     /
 \    |.|    /
  \   |f|   /
   \  |u|  /
    |ta|s|pe|
    |ta|e|pe|
      |.|
      |f|
      |u|
      |s|
      |e|
      |.|
      |_|
```

The match book is wrapped around the matches, and is taped to itself. The matches are taped to the fuse. The striker will rub against the matcheads when the match book is pulled.

6) When ready to use, simply pull on the match paper. It should pull the striking paper across the match heads with enough friction to light them. In turn, the burning matcheads will light the fuse, since it adjacent to the burning match heads.

4.22 IMPACT IGNITION

Impact ignition is an excellent method of ignition for spontaneous terrorist activities. The problem with an impact-detonating device is that it must be kept in a very safe container so that it will not explode while being transported to the place where it is to be used. This can be done by having a removable impact initiator.

The best and most reliable impact initiator is one that uses factory made initiators or primers. A no. 11 cap for black powder firearms is one such primer. They usually come in boxes of 100, and cost about $2.50. To use such a cap, however, one needs a nipple that it will fit on. Black powder nipples are also available in gun stores. All that a person has to do is ask for a package of nipples and the caps that fit them. Nipples have a hole that goes all the way through them, and they have a threaded end, and an end to put the cap on. A cutaway of a nipple is shown below:

```
            |          |
            _           |
           | |           |
      _________| |^^^^^^^^^|      |
      |    ____________|      |
      |   |             |
no. 11     |________|           |
percussion   ________           | ------- threads for screwing
cap here   |    |          |      nipple onto bomb
      |   |____________      |
      |________     |     |
          | |^^^^^^^^^^|     |
          |_|          |
                     |
            |__________________|
```

When making using this type of initiator, a hole must be drilled into whatever container is used to make the bomb out of. The nipple is then screwed into the hole so that it fits tightly. Then, the cap can be carried and placed on the bomb when it is to be thrown. The cap should be bent a small amount before it is placed on the nipple, to make sure that it stays in place. The only other problem involved with an impact detonating bomb is that it must strike a hard surface on the nipple to set it off. By attaching fins or a small parachute on the end of the bomb opposite the primer, the bomb, when thrown, should strike the ground on the primer, and explode. Of course, a bomb with mercury fulminate in each end will go off on impact regardless of which end it strikes on, but mercury fulminate is also likely to go off if the person carrying the bomb is bumped hard.

4.23 ELECTRICAL IGNITION

Electrical ignition systems for detonation are usually the safest and most reliable form of ignition. Electrical systems are ideal for demolition work, if one doesn't have to worry so much about being caught. With two spools of 500 ft of wire and a car battery, one can detonate explosives from a "safe", comfortable distance, and be sure that there is nobody around that could get hurt. With an electrical system, one can control exactly what time a device will explode, within fractions of a second. Detonation can be aborted in less than a second's warning, if a person suddenly walks by the detonation sight, or if a police car chooses to roll by at the time. The two best electrical igniters are military squibs and model rocketry igniters. Blasting caps for construction also work well. Model rocketry igniters are sold in packages of six, and cost about $1.00 per pack. All that need be done to use them is connect it to two wires and run a current through them. Military squibs are difficult to get, but they are a little bit better, since they explode when a current is run through them, whereas rocketry igniters only burst into flame. Military squibs can be used to set off sensitive high explosives, such as R.D.X., or potassium chlorate mixed with petroleum jelly. Igniters can be used to set off black powder, mercury fulminate, or guncotton, which in turn, can set of a high order explosive.

4.24 ELECTRO-MECHANICAL IGNITION

Electro-mechanical ignition systems are systems that use some type of mechanical switch to set off an explosive charge electrically. This type of switch is typically used in booby traps or other devices in which the person who places the bomb does not wish to be anywhere near the device when it explodes. Several types of electro-mechanical detonators will be discussed.

4.241 Mercury Switches

Mercury switches are a switch that uses the fact that mercury metal conducts electricity, as do all metals, but mercury metal is a liquid at room temperatures. A typical mercury switch is a sealed glass tube with two electrodes and a bead of mercury metal. It is sealed because of mercury's nasty habit of giving off brain-damaging vapors. The diagram below may help to explain a mercury switch.

```
                  _______________
               A  /           \  B
   _____wire +______/____________    \
                \  ( Hg )  |   /
                 \ _(_Hg_)__|___/
                          |
                          |
                   wire - |
                          |
                          |
```

When the drop of mercury ("Hg" is mercury's atomic symbol) touches both contacts, current flows through the switch. If this particular switch was in its present position, A---B, current would be flowing, since the mercury can touch both contacts in the horizontal position.

If, however, it was in the | position, the drop of mercury would only touch the + contact on the A side. Current, then couldn't flow, since mercury does not reach both contacts when the switch is in the vertical position.

This type of switch is ideal to place by a door. If it were placed in the path of a swinging door in the verticle position, the motion of the door would knock the switch down, if it was held to the ground by a piece if tape. This would tilt the switch into the verticle position, causing the mercury to touch both contacts, allowing current to flow through the mercury, and to the igniter or squib in an explosive device. Imagine opening a door and having it slammed in your face by an explosion.

4.242 Tripwire Switches

A tripwire is an element of the classic booby trap. By placing a nearly invisible line of string or fishing line in the probable path of a victim, and by putting some type of trap there also, nasty things can be caused to occur. If this mode of thought is applied to explosives, how would one use such a tripwire to detonate a bomb. The technique is simple. By wrapping the tips of a standard clothespin with aluminum foil, and placing something between them, and connecting wires to each aluminum foil contact, an electric tripwire can be made, If a piece of wood attached to the tripwire was placed between the contacts on the clothespin, the clothespin would serve as a switch. When the tripwire was pulled, the clothespin would snap together, allowing current to flow between the two pieces of aluminum foil, thereby completing a circuit, which would have the igniter or squib in it. Current would flow between the contacts to the igniter or squib, heat the igniter or squib, causing it it to explode.

```
                    ____________________________________
                    \_foil____________________________/
 Insert strip of       ---------------------------spring
 wood with trip-       _foil___________________________
 wire between foil   /________________________________\
 contacts.
```

Make sure that the aluminum foil contacts do not touch the spring, since the spring also conducts electricity.

4.243 Radio Control Detonators

In the movies, every terrorist or criminal uses a radio controlled detonator to set off explosives. With a good radio detonator, one can be several miles away from the device, and still control exactly when it explodes, in much the same way as an electrical switch. The problem with radio detonators is that they are rather costly. However, there could possibly be a reason that a terrorist would wish to spend the amounts of money involved with a RC (radio control) system and use it as a detonator. If such an individual wanted to devise an RC detonator, all he would need to do is visit the local hobby store or toy store, and buy a radio controlled toy. Taking it back to his/her abode, all that he/she would have to do is detach the solenoid/motor that controls the motion of the front wheels of a RC car, or detach the solenoid/motor of the elevators/rudder of a RC plane, or the rudder of a RC boat, and re-connect the squib or rocket engine igniter to the contacts for the solenoid/motor. The device should be tested several times with squibs or igniters, and fully charged batteries should be in both the controller and the receiver (the part that used to move parts before the device became a detonator).

4.3 DELAYS

A delay is a device which causes time to pass from when a device is set up to the time that it explodes. A regular fuse is a delay, but it would cost quite a bit to have a 24 hour delay with a fuse. This section deals with the different types of delays that can be employed by a terrorist who wishes to be sure that his bomb will go off, but wants to be out of the country when it does.

4.31 FUSE DELAYS

It is extremely simple to delay explosive devices that employ fuses for ignition. Perhaps the simplest way to do so is with a cigarette. An average cigarette burns for about 8 minutes. The higher the "tar" and nicotine rating, the slower the cigarette burns. Low "tar" and nicotine cigarettes burn quicker than the higher "tar" and nicotine cigarettes, but they are also less likely to go out if left unattended, i.e. not smoked. Depending on the wind or draft in a given place, a high "tar" cigarette is better for delaying the ignition of a fuse, but there must be enough wind or draft to give the cigarette enough oxygen to burn. People who use cigarettes for the purpose of delaying fuses will often test the cigarettes that they plan to use in advance to make sure they stay lit and to see how long it will burn. Once a cigarettes burn rate is determined, it is a simple matter of carefully putting a hole all the way through a cigarette with a toothpick at the point desired, and pushing the fuse for a device in the hole formed.

```
                    |=|
                    |=| ---------- filter
                    |=|
                    | |
                    | |
                    |o| ---------- hole for fuse
 cigarette ------------    | |
                    | |
                    | |
                    | |
                    | |
                    | |
                    | |
                    | |
                    | |
                    |_| ---------- light this end
```

A similar type of device can be make from powdered charcoal and a sheet of paper. Simply roll the sheet of paper into a thin tube, and fill it with powdered charcoal. Punch a hole in it at the desired location, and insert a fuse. Both ends must be glued closed, and one end of the delay must be doused with lighter fluid before it is lit. Or, a small charge of gunpowder mixed with powdered charcoal could conceivably used for igniting such a delay. A chain of charcoal briquettes can be used as a delay by merely lining up a few bricks of charcoal so that they touch each other, end on end, and lighting the first brick. Incense, which can be purchased at almost any novelty or party supply store, can also be used as a fairly reliable delay. By wrapping the fuse about the end of an incense stick, delays of up to 1/2 an hour are possible.

Finally, it is possible to make a relatively slow-burning fuse in the home. By dissolving about one teaspoon of black powder in about 1/4 a cup of boiling water, and, while it is still hot, soaking in it a long piece of all cotton string, a slow-burning fuse can be made. After the soaked string dries, it must then be tied to the fuse of an explosive device. Sometimes, the end of the slow burning fuse that meets the normal fuse has a charge of black powder or gunpowder at the intersection point to insure ignition, since the slow-burning fuse does not burn at a very high temperature. A similar type of slow fuse can be made by taking the above mixture of boiling water and black powder and pouring it on a long piece of toilet paper. The wet toilet paper is then gently twisted up so that it resembles a firecracker fuse, and is allowed to dry.

4.32 TIMER DELAYS

Timer delays, or "time bombs" are usually employed by an individual who wishes to threaten a place with a bomb and demand money to reveal its location and means to disarm it. Such a device could be placed in any populated place if it were concealed properly. There are several ways to build a timer delay. By simply using a screw as one contact at the time that detonation is desired, and using the hour hand of a clock as the other contact, a simple timer can be made. The minute hand of a clock should be removed, unless a delay of less than an hour is desired.

```
        _________________________________________  to igniter    from
igniter
        |                    |
        |        12           |   :       :
        |     11       1       |   :       :
        |                    |   :       :
        |   10            2    |   :       :
        |          o...............|......:       :
        |                    |           :
        |  9               3   |           :
        |                    |           :
        |                    |           :
        |   8             4    |           :
        |              o.........|......       :
        |      7        5      |   :       :
        |          6          |   :.+.....-.....:
        |________________________________________|   __|_____|
                        |       |
                        | battery |
    o - contacts            |       |
    ..... - wire           |       |
                        |____________|
```

This device is set to go off in eleven hours. When the hour hand of the clock reaches the contact near the numeral 5, it will complete the circuit, allowing current to flow through the igniter or squib.

The main disadvantage with this type of timer is that it can only be set for a maximum time of 12 hours. If an electronic timer is used, such as that in an electronic clock, then delays of up to 24 hours are possible. By removing the speaker from an electronic clock, and attaching the wires of a squib or igniter to them, a timer with a delay of up to 24 hours can be made. To utilize this type of timer, one must have a socket that the clock can be plugged into. All that one has to do is set the alarm time of the clock to the desired time, connect the leads, and go away. This could also be done with an electronic watch, if a larger battery were used, and the current to the speaker of the watch was stepped up via a transformer. This would be good, since such a timer could be extremely small. The timer in a VCR (Video Cassette Recorder) would be ideal. VCR's can usually be set for times of up to a week. The leads from the timer to the recording equipment would be the ones that an igniter or squib would be connected to. Also, one can buy timers from electronics stores that would be ideal. Finally, one could employ a digital watch, and use a relay, or electro-magnetic switch to fire the igniter, and the current of the watch would not have to be stepped up.

4.33 CHEMICAL DELAYS

Chemical delays are uncommon, but they can be extremely effective in some cases. If a glass container is filled with concentrated sulfuric acid, and capped with several thicknesses of aluminum foil, or a cap that it will eat through, then it can be used as a delay. Sulfuric acid will react with aluminum foil to produce aluminum sulfate and hydrogen gas, and so the container must be open to the air on one end so that the pressure of the hydrogen gas that is forming does not break the container. See diagram on following page.

```
 _           _
| |         | |
| |         | |
| |         | |
| |_____________| |
| |         | |
| |  sulfuric   | |
| |         | |
| |  acid      | |
| |         | |---------- aluminum foil
| |_____________| |          (several thicknesses)
|_________________|
```

The aluminum foil is placed over the bottom of the container and secured there with tape. When the acid eats through the aluminum foil, it can be used to ignite an explosive device in several ways.

1) Sulfuric acid is a good conductor of electricity. If the acid that eats through the foil is collected in a glass container placed underneath the foil, and two wires are placed in the glass container,
 a current will be able to flow through the acid when both of the wires are immersed in the acid.

2) Sulfuric acid reacts very violently with potassium chlorate. If

the acid drips down into a container containing potassium chlorate, the potassium chlorate will burst into flame. This flame can be used to ignite a fuse, or the potassium chlorate can be the igniter for a thermit bomb, if some potassium chlorate is mixed in a 50/50 ratio with the thermit, and this mixture is used as an igniter for the rest of the thermit.

3) Sulfuric acid reacts with potassium permangenate in a similar way.

4.4 EXPLOSIVE CONTAINERS

This section will cover everything from making a simple firecracker to a complicated scheme for detonating an insensitive high explosive, both of which are methods that could be utilized by perpetrators of terror.

4.41 PAPER CONTAINERS

Paper was the first container ever used for explosives, since it was first used by the Chinese to make fireworks. Paper containers are usually very simple to make, and are certainly the cheapest. There are many possible uses for paper in containing explosives, and the two most obvious are in firecrackers and rocket engines. Simply by rolling up a long sheet of paper, and gluing it together, one can make a simple rocket engine. Perhaps a more interesting and dangerous use is in the firecracker. The firecracker shown here is one of Mexican design. It is called a "polumna", meaning "dove". The process of their manufacture is not unlike that of making a paper football. If one takes a sheet of paper about 16 inches in length by 1.5 inches wide, and fold one corner so that it looks like this:

```
 ______________________________________________________
|                          |\
|                          | \
|                          |  \
|_____________________________________________________|___\
```

and then fold it again so that it looks like this:

```
 _____________________________________________________
|                          /|
|                         / |
|                        /  |
|________________________________________________/___|
```

A pocket is formed. This pocket can be filled with black powder, pyrodex, flash powder, gunpowder,rocket engine powder, or any of the quick-burning fuel- oxodizer mixtures that occur in the form of a fine powder. A fuse is then inserted, and one continues the triangular folds, being careful not to spill out any of the explosive. When the polumna is finished, it should be taped together very tightly, since this will increase the strength of the container, and produce a louder and more powerful explosion when it is lit. The finished polumna should look like a 1/4 inch - 1/3 inch thick triangle, like the one shown below:

```
          ^
         / \  ----- securely tape all corners
        /   \
       /     \
      /       \
     /         \
    /           \______________________________
   /_______________\__/__/__/__/__/__/__/__/__/__/  ---------- fuse
```

4.42 METAL CONTAINERS

The classic pipe bomb is the best known example of a metal-contained explosive. Idiot anarchists take white tipped matches and cut off the match heads. They pound one end of a pipe closed with a hammer, pour in the white- tipped matches, and then pound the other end closed. This process often kills the fool, since when he pounds the pipe closed, he could very easily cause enough friction between the match heads to cause them to ignite and explode the unfinished bomb. By using pipe caps, the process is somewhat safer, and the less stupid anarchist would never use white tipped matches in a bomb. He would buy two pipe caps and threaded pipe (fig. 1). First, he would drill a hole in one pipe cap, and put a fuse in it so that it will not come out, and so powder will not escape during handling. The fuse would be at least 3/4 an inch long inside the bomb. He would then screw the cap with the fuse in it on tightly, possibly putting a drop of super glue on it to hold it tight. He would then pour his explosive powder in the bomb. To pack it tightly, he would take a large wad of tissue paper and, after filling the pipe to the very top, pack the powder down, by using the paper as a ramrod tip, and pushing it with a pencil or other wide ended object, until it would not move any further. Finally, he would screw the other pipe cap on, and glue it. The tissue paper would help prevent some of the powder from being caught in the threads of the pipe or pipe cap from being crushed and subject to friction, which might ignite the powder, causing an explosion during manufacture. An assembled bomb is shown in fig. 2.

```
 __________       _________________        ___________
 |      |    ^^^^^^            ^^^^^^    |       |
 | |vvvvv|   |____________________________|    |vvvvvv| |
 | |                                    | |
 | |                                    | |
 | |                                    | |
| |                                              | |
| |          ______________________________           | |
| |         |                    |         | |
| |^^^^^|     vvvvvv________________vvvvvv    |^^^^^^| |
|_______|                              |________|
```

fig 1. Threaded pipe and endcaps.

```
    ________                           ________
    | _____|__________________________________|_____ |
    | |_____________________________________________| |
    | |: : : : |- - - - - - - - - - - - - - - - -| |
    | | tissue | - - - - - - - - - - - - - - - - |_|
    | | : : :  |- - - low order explosive - - ----------------------
    | | paper  | - - - - - - - - - - - - - - - - |-|    fuse
    | |: : : : |- - - - - - - - - - - - - - - - -| |
    | |________|___________________________________| |
    | |_____________________________________________| |
    |______|                          |______|

    endcap              pipe              endcap
                                      w/ hole
```

fig. 2 Assembled pipe bomb.

This is one possible design that a mad bomber would use. If, however, he did not have access to threaded pipe with endcaps, he could always use a piece of copper or aluminum pipe, since it is easily bent into a suitable position. A major problem with copper piping, however, is bending and folding it without tearing it; if too much force is used when folding and bending copper pipe, it will split along the fold. The safest method for making a pipe bomb out of copper or aluminum pipe is similar to the method with pipe and endcaps. First, one flattens one end of a copper or aluminum pipe carefully, making sure not to tear or rip the piping. Then, the flat end of the pipe should be folded over at least once, if this does not rip the pipe. A fuse hole should be drilled in the pipe near the now closed end, and the fuse should be inserted. Next, the bomb-builder would fill the bomb with a low order explosive, and pack it with a large wad of tissue paper. He would then flatten and fold the other end of the pipe with a pair of pliers. If he was not too dumb, he would do this slowly, since the process of folding and bending metal gives off heat, which could set off the explosive. A diagram is presented below:

```
                                    ________
 ________________________________________________/      |
 |                                      |
 |                                   o  |
 |_______________________________________________       |
                                  \_______|
```

fig. 1 pipe with one end flattened and fuse hole drilled (top view)

```
                                  ______
 _____________________________________________/  | |
 |                                  | |
 |                                o | |
 |____________________________________________   | |
                                \__|__|
```

fig. 2 pipe with one end flattened and folded up (top view)

```
                  ____________ fuse hole
                  |
                  v
 __________________________________________________
 |                      \ |____ |
 |                       \____| |
 |                        ______|
 |                       /
 |______________________________/__________________
```

fig. 3 pipe with flattened and folded end (side view)

```
                               _________________ fuse
                              /
                              |
  ________    _____________________________|___   ________
  |  ____|  /    |- - - - - - - - - - -| - -  \  |___  |
  |  |_____/tissue| - - - - - - - - - - - -|- - \_____| |
  |________ paper |- - -  low order explosive -  _______|
      \       | - - - - - - - - - - - - - - /
       \______________________________________/
```

fig. 4 completed bomb, showing tissue paper packing and explosive
          (side view)

A CO2 cartridge from a B.B gun is another excellent container for a low-order explosive. It has one minor disadvantage: it is time consuming to fill. But this can be rectified by widening the opening of the cartridge with a pointed tool. Then, all that would have to be done is to fill the CO2 cartridge with any low-order explosive, or any of the fast burning fuel- oxodizer mixtures, and insert a fuse. These devices are commonly called "crater makers".

A CO2 cartridge also works well as a container for a thermit incendiary device, but it must be modified. The opening in the end must be widened, so that the ignition mixture, such as powdered magnesium, does not explode. The fuse will ignite the powdered magnesium, which, in turn, would ignite the thermit.

The previously mentioned designs for explosive devices are fine for low-order explosives, but are unsuitable for high-order explosives, since the latter requires a shockwave to be detonated. A design employing a smaller low-order explosive device inside a larger device containing a high-order explosive would probably be used. It would look something like:

```
                          _______________________ fuse
                          |
                          |
                          |
 _________                |         _________
 |  ____|_________________________|___________|____   |
 |  |* * * * * * * * * * * * * * *|* * * * * * *  |  |
 |  | * * * * * *  high explosive | * * * * * * * |  |
 |  |* * * * * * * * * * * * * * *|* * * * * * *  |  |
 |  | *  ______     _______________|_    ______  * |  |
 |  |* * |  __|  /   - - - - - - | \  |__  |*  |  |
 |  | *  |  |____/   low explosive - \____|  |  * |  |
 |  |* * |_______  - - - - - - - - -  _______| *  |  |
 |  | * * * * * \ - - - - - - - - / * * * * *|  |
 |  |* * * * * * \_________________/ * * * * *  |  |
 |  | * * * * * * * * * * * * * * * * * * * * * *|  |
 |  |* * * * * * * * * * * * * * * * * * * * * *  |  |
 |  | * * * * * * * * * * * * * * * * * * * * * *|  |
 |  |______________________________________________|  |
 |_______|                          |_______|
```

If the large high explosive container is small, such as a CO2 cartridge, then a segment of a hollow radio antenna can be made into a low-order pipe bomb, which can be fitted with a fuse, and inserted into the CO2 cartridge.

4.43 GLASS CONTAINERS

Glass containers can be suitable for low-order explosives, but there are problems with them. First, a glass container can be broken relatively easily compared to metal or plastic containers. Secondly, in the not-too-unlikely event of an "accident", the person making the device would probably be seriously injured, even if the device was small. A bomb made out of a sample perfume bottle-sized container exploded in the hands of one boy, and he still has pieces of glass in his hand. He is also missing the final segment of his ring finger, which was cut off by a sharp piece of flying glass...

Nonetheless, glass containers such as perfume bottles can be used by a demented individual, since such a device would not be detected by metal detectors in an airport or other public place. All that need be done is fill the container, and drill a hole in the plastic cap that the fuse fits tightly in, and screw the cap-fuse assembly on.

```
           _________________________  fuse
           |
           |
           |
      _____|_____
      | ___|___ |
      | >  |  < |  drill hole in cap, and insert fuse;
      | >  |  < |  be sure fuse will not come out of cap
      | >  |  < |
      |    |    |
      |         |
      |         |
      |         |  screw cap on bottle
      |         |
      |         |
      V         V


        _________
       <         >
       <         >
       <         >
         /     \
        /       \
       /         \
      |           |  fill bottle with low-order explosive
      |           |
      |           |
      |           |
      |           |
      |___________|
```

Large explosive devices made from glass containers are not practicle, since glass is not an exceptionally strong container. Much of the explosive that is used to fill the container is wasted if the container is much larger than a 16 oz. soda bottle. Also, glass containers are usually unsuitable for high explosive devices, since a glass container would probably not withstand the explosion of the initiator; it would shatter before the high explosive was able to detonate.

4.44 PLASTIC CONTAINERS

Plastic containers are perhaps the best containers for explosives, since they can be any size or shape, and are not fragile like glass. Plastic piping can be bought at hardware or plumbing stores, and a device much like the ones used for metal containers can be made. The high-order version works well with plastic piping. If the entire device is made out of plastic, it is not detectable by metal detectors. Plastic containers can usually be shaped by heating the container, and bending it at the appropriate place. They can be glued closed with epoxy or other cement for plastics. Epoxy alone can be used as an endcap, if a wad of tissue paper is placed in the piping. Epoxy with a drying agent works best in this type of device.

```
||             ||
||             ||
||\_______________/||
||             ||
||    epoxy    ||
||_________________||
||             ||
||   tissue    ||
||    paper    ||
||_________________||
||***************||
||***************||
||***************||
||***************||
||** explosive **||
||***************||
||***********-----------------------  fuse
||***************||
||---------------||
||             ||
||   tissue    ||
||    paper    ||
||_________________||
||             ||
||    epoxy    ||
|| _______________ ||
||/            \||
||             ||
||             ||
```

One end must be made first, and be allowed to dry completely before the device can be filled with powder and fused. Then, with another piece of tissue paper, pack the powder tightly, and cover it with plenty of epoxy. PVC pipe works well for this type of device, but it cannot be used if the pipe had an inside diameter greater than 3/4 of an inch. Other plastic puttys can be used int this type of device, but epoxy with a drying agent works best.

4.5 ADVANCED USES FOR EXPLOSIVES

The techniques presented here are those that could be used by a person who had some degree of knowledge of the use of explosives. Some of this information comes from demolitions books, or from military handbooks. Advanced uses for explosives usually involved shaped charges, or utilize a minimum amount of explosive to do a maximum amount of damage. They almost always involve high- order explosives.

4.51 SHAPED CHARGES

A shaped charge is an explosive device that, upon detonation, directs the explosive force of detonation at a small target area. This process can be used to breach the strongest armor, since forces of literally millions of pounds of pressure per square inch can be generated. Shaped charges employ high-order explosives, and usually electric ignition systems. KEEP IN MIND THAT ALL EXPLOSIVES ARE DANGEROUS, AND SHOULD NEVER BE MADE OR USED!!

An example of a shaped charge is shown below.

```
              + wire _________         ________ - wire
                             |       |
                             |       |
                             |       |
 _                  __________|__________|_____________
 ^                 | _________|__________|___________ |
 |                 | |      |        |        | |
 |                 | |      \ igniter /        | |
 |                 | |       \_______/         | |
 |                 | |    priming charge       | |
 |                 | |  (mercury fulminate)    | |
 |                 | |           ^             | |
 |                 | |          / \            | |
 |                 | |         /   \           | |
 |                 | |        /     \          | |
 |                 | |       /       \         | |
 |                 | |      /         \        | |
 |                 | |     /           \       | |
                   | |    /             \      | |
 8 inches high        | |   /               \     | |
                   | |   /      high      \   | |
 |                 | |  /     explosive    \  | |
 |                 | | /       charge       \ | |
 |                 | |/                      \| |
 |                 | |/                      \| |
 |                 | |           ^             | |
 |                 | |          / \            | |
 |                 | |         /   \           | |
 |                 | |        /     \          | |
 |                 | |       /       \         | |
 |               | |      /       \      | |
 |               | |     /         \     | |
 |               | |    /           \    | |
 |               | |   /             \   | |
 |               | |  /               \  | | ------- 1/2 inch
 |               | | /                 \ | |       thick
steel
 |               | |/                   \| |       pipe
 |               | /                     \ |
 |               | |/                    \| |
 |    hole for   | |                     | |    hole for
 |    screw      | |                     | |     screw
 |               | |                     | |
 V_______   ___________| |               | |___________
________
 |______|  |____________|                |____________|
|______|

                 |<------- 8 inches -------->|
```

If a device such as this is screwed to a safe, for example, it would direct most of the explosive force at a point about 1 inch away from the opening of the pipe. The basis for shaped charges is a cone-shaped opening in the explosive material. This cone should have an angle of 45 degrees. A device such as this one could also be attached to a metal surface with a powerful electromagnet.

4.52   TUBE EXPLOSIVES

A variation on shaped charges, tube explosives can be used in ways that shaped charges cannot. If a piece of 1/2 inch plastic tubing was filled with a sensitive high explosive like R.D.X., and prepared as the plastic explosive container in section 4.44, a different sort of shaped charge could be produced; a charge that directs explosive force in a circular manner. This type of explosive could be wrapped around a column, or a doorknob, or a telephone pole. The explosion would be directed in and out, and most likely destroy whatever it was wrapped around. In an unbent state, a tube explosive would look like this:

```
||      ||
||      ||
||\____/||
|| epoxy||
||______||
||      ||
||tissue||
|| paper||
||______||
||******||
||******||
||******||
||******||
||******||
||******||
||******||
||******||
|| RDX  ||
||******||
||******||
||******||
||******||
|| ____ ||
|| | s| ||
|| | q| ||
|| | u| ||
|| | i| ||
|| | b| ||
|| | b| ||
|| |__| ||
||__||__||
||tissue||
|| paper||
||__||__||
||  ||  ||
|| epoxy||
||  ||  ||
|| _||_ ||
||/ || \||
||  ||  ||
||  ||  ||
    ||_______ + wire ______________
    |
    |________ - wire ______________
```

When an assassin or terrorist wishes to use a tube bomb, he must wrap it around whatever thing he wishes to destroy, and epoxy the ends of the tube bomb together. After it dries, he/she can connect wires to the squib wires, and detonate the bomb, with any method of electric detonation.

4.53 ATOMIZED PARTICLE EXPLOSIONS

If a highly flammable substance is atomized, or, divided into very small particles, and large amounts of it is burned in a confined area, an explosion similar to that occurring in the cylinder of an automobile is produced. The tiny droplets of gasoline burn in the air, and the hot gasses expand rapidly, pushing the cylinder up. Similarly, if a gallon of gasoline was atomized and ignited in a building, it is very possible that the expanding gassed would push the walls of the building down. This phenomenon is called an atomized particle explosion. If a person can effectively atomize a large amount of a highly flammable substance and ignite it, he could bring down a large building, bridge, or other structure. Atomizing a large amount of gasoline, for example, can be extremely difficult, unless one has the aid of a high explosive. If a gallon jug of gasoline was placed directly over a high explosive charge, and the charge was detonated, the gasoline would instantly be atomized and ignited. If this occurred in a building, for example, an atomized particle explosion would surely occur. Only a small amount of high explosive would be necessary to accomplish this feat, about 1/2 a pound of T.N.T. or 1/4 a pound of R.D.X. Also, instead of gasoline, powdered aluminum could be used. It is necessary that a high explosive be used to atomize a flammable material, since a low-order explosion does not occur quickly enough to atomize or ignite the flammable material.

4.54 LIGHTBULB BOMBS

An automatic reaction to walking into a dark room is to turn on the light. This can be fatal, if a lightbulb bomb has been placed in the overhead light socket. A lightbulb bomb is surprisingly easy to make. It also comes with its own initiator and electric ignition system. On some lightbulbs, the lightbulb glass can be removed from the metal base by heating the base of a lightbulb in a gas flame, such as that of a blowtorch or gas stove. This must be done carefully, since the inside of a lightbulb is a vacuum. When the glue gets hot enough, the glass bulb can be pulled off the metal base. On other bulbs, it is necessary to heat the glass directly with a blowtorch or oxy-acetylene torch. When the bulb is red hot, a hole must be carefully poked in the bulb, remembering the vacuum state inside the bulb. In either case, once the bulb and/or base has cooled down to room temperature or lower, the bulb can be filled with an explosive material, such as black powder. If the glass was removed from the metal base, it must be glued back on to the base with epoxy. If a hole was put in the bulb, a piece of duct tape is sufficient to hold the explosive in the in the bulb. Then, after making sure that the socket has no power by checking with a working lightbulb, all that need be done is to screw the lightbulb bomb into the socket. Such a device has been used by terrorists or assassins with much success, since nobody can search the room for a bomb without first turning on the light.

4.55 BOOK BOMBS

Concealing a bomb can be extremely difficult in a day and age where perpetrators of violence run wild. Bags and briefcases are often searched by authorities whenever one enters a place where an individual might intend to set off a bomb. One approach to disguising a bomb is to build what is called a book bomb; an explosive device that is entirely contained inside of a book. Usually, a relatively large book is required, and the book must be of the hardback variety to hide any protrusions of a bomb. Dictionaries, law books, large textbooks, and other such books work well. When an individual makes a bookbomb, he/she must choose a type of book that is appropriate for the place where the book bomb will be placed. The actual construction of a book bomb can be done by anyone who possesses an electric drill and a coping saw. First, all of the pages of the book must be glued together. By pouring an entire container of water-soluble glue into a large bucket, and filling the bucket with boiling water, a glue-water solution can be made that will hold all of the book's pages together tightly. After the glue-water solution has cooled to a bearable temperature, and the solution has been stirred well, the pages of the book must be immersed in the glue-water solution, and each page must be thoroughly soaked. It is extremely important that the covers of the book do not get stuck to the pages of the book while the pages are drying. Suspending the book by both covers and clamping the pages together in a vice works best. When the pages dry, after about three days to a week, a hole must be drilled into the now rigid pages, and they should drill out much like wood. Then, by inserting the coping saw blade through the pages and sawing out a rectangle from the middle of the book, the individual will be left with a shell of the book's pages. The pages, when drilled out, should look like this:

```
 ________________________
| ____________________ |
| |          | |
| |          | |
| |          | |
| |          | |
| |          | |
| |          | |
| |          | |
| |          | |
| |          | |
| |          | |
| |          | |
| |__________________| |
|______________________|
```

(book covers omitted)

This rectangle must be securely glued to the back cover of the book. After building his/her bomb, which usually is of the timer or radio controlled variety, the bomber places it inside the book. The bomb itself, and whatever timer or detonator is used, should be packed in foam to prevent it from rolling or shifting about. Finally, after the timer is set, or the radio control has been turned on, the front cover is glued closed, and the bomb is taken to its destination.

4.56 PHONE BOMBS

The phone bomb is an explosive device that has been used in the past to kill or injure a specific individual. The basic idea is simple: when the person answers the phone, the bomb explodes. If a small but powerful high explosive device with a squib was placed in the phone receiver, when the current flowed through the receiver, the squib would explode, detonating the high explosive in the person's hand. Nasty. All that has to be done is acquire a squib, and tape the receiver switch down. Unscrew the mouthpiece cover, and remove the speaker, and connect the squib's leads where it was. Place a high explosive putty, such as C-1 (see section 3.31) in the receiver, and screw the cover on, making sure that the squib is surrounded by the C-1. Hang the phone up, and leave the tape in place. When the individual to whom the phone belongs attempts to answer the phone, he will notice the tape, and remove it. This will allow current to flow through the squib. Note that the device will not explode by merely making a phone call; the owner of the phone must lift up the receiver, and remove the tape. It is highly probable that the phone will be by his/her ear when the device explodes...

5.0 SPECIAL AMMUNITION FOR PROJECTILE WEAPONS

Explosive and/or poisoned ammunition is an important part of a social deviant's arsenal. Such ammunition gives the user a distinct advantage over individual who use normal ammunition, since a grazing hit is good enough to kill. Special ammunition can be made for many types of weapons, from crossbows to shotguns.

5.1 SPECIAL AMMUNITION FOR PRIMITIVE WEAPONS

For the purposes of this publication, we will call any weapon primitive that does not employ burning gunpowder to propel a projectile forward. This means blowguns, bows and crossbows, and wristrockets.

5.11 BOW AND CROSSBOW AMMUNITION

Bows and crossbows both fire arrows or bolts as ammunition. It is extremely simple to poison an arrow or bolt, but it is a more difficult matter to produce explosive arrows or bolts. If, however, one can acquire aluminum piping that is the same diameter of an arrow or crossbow bolt, the entire segment of piping can be converted into an explosive device that detonates upon impact, or with a fuse. All that need be done is find an aluminum tube of the right length and diameter, and plug the back end with tissue paper and epoxy. Fill the tube with any type of low-order explosive or sensitive high- order explosive up to about 1/2 an inch from the top. Cut a slot in the piece of tubing, and carefully squeeze the top of the tube into a round point, making sure to leave a small hole. Place a no. 11 percussion cap over the hole, and secure it with super glue. Finally, wrap the end of the device with electrical or duct tape, and make fins out of tape. Or, fins can be bought at a sporting goods store, and glued to the shaft. The finished product should look like:

```
 _____
|   | ---------- no. 11 percussion cap
||*||
 |*|
 |*|
 |*|
        |*|
        |*|
        |*| ----------- aluminum piping
        |*|
        |e|
        |x|
        |p|
        |l|
        |o|
        |s|
        |i|
        |v|
        |e|
        |*|
        |*|
        |*|
        |*|
        |*|
        |*|
        |*|
       /|_|\
      / |t| \
      | |p| |
      | |_| |
      | |e| | --------- fins
      | |p| |
      | |y| |
      |_|_|_|
        |_|
```

tp: tissue paper

epy: epoxy

When the arrow or bolt strikes a hard surface, the percussion cap explodes, igniting or detonating the explosive.

5.12 SPECIAL AMMUNITION FOR BLOWGUNS

The blowgun is an interesting weapon which has several advantages. A blowgun can be extremely ccurate, concealable, and deliver an explosive or poisoned projectile. The manufacture of an explosive dart or projectile is not difficult. Perhaps the most simple design for such involves the use of a pill capsule, such as the kind that are taken for headaches or allergies.

Such a capsule could easily be opened, and the medicine removed. Next, the capsule would be re-filled with an impact-sensitive explosive. An additional high explosive charge could be placed behind the impact-sensitive explosive, if one of the larger capsules were used. Finally, the explosive capsule would be reglued back together, and a tassel or cotton would be glued to the end containing the high explosive, to insure that the impact-detonating explosive struck the target first. Such a device would probably be about 3/4 of an inch long, not including the tassel or cotton, and look something like this:

```
    ______________________
   /mercury |          \----------------------
  (fulminate|   R.D.X.   )--------------------- } tassels
   \_________|____________/----------------------
```

5.13   SPECIAL AMMUNITION FOR WRISTROCKETS AND SLINGSHOTS

A modern wristrocket is a formidable weapon. It can throw a shooter marble about 500 ft. with reasonable accuracy. Inside of 200 ft., it could well be lethal to a man or animal, if it struck in a vital area. Because of the relatively large sized projectile that can be used in a wristrocket, the wristrocket can be adapted to throw relatively powerful explosive projectiles. A small segment of aluminum pipe could be made into an impact-detonating device by filling it with an impact-sensitive explosive material. Also, such a pipe could be filled with a low-order explosive, and fitted with a fuse, which would be lit before the device was shot. One would have to make sure that the fuse was of sufficient length to insure that the device did not explode before it reached its intended target. Finally, .22 caliber caps, such as the kind that are used in .22 caliber blank guns, make excellent exploding ammunition for wristrockets, but they must be used at a relatively close range, because of their light weight.

5.2   SPECIAL AMMUNITION FOR FIREARMS

When special ammunition is used in combination with the power and rapidity of modern firearms, it becomes very easy to take on a small army with a single weapon. It is possible to buy explosive ammunition, but that can be difficult to do. Such ammunition can also be manufactured in the home. There is, however, a risk involved with modifying any ammunition. If the ammunition is modified incorrectly, in such a way that it makes the bullet even the slightest bit wider, an explosion in the barrel of the weapon will occur. For this reason, NOBODY SHOULD EVER ATTEMPT TO MANUFACTURE SUCH AMMUNITION.

5.21   SPECIAL AMMUNITION FOR HANDGUNS

If an individual wished to produce explosive ammunition for his/her handgun, he/she could do it, provided that the person had an impact-sensitive explosive and a few simple tools. One would first purchase all lead bullets, and then make or acquire an impact-detonating explosive. By drilling a hole in a lead bullet with a drill, a space could be created for the placement of an explosive. After filling the hole with an explosive, it would be sealed in the bullet with a drop of hot wax from a candle. A diagram of a completed exploding bullet is shown below.

```
   _o_ ------------ drop of wax
  /|*|\
 | |*|-|----------- impact-sensitive explosive
 | |_| |
 |_____|
```

This hollow space design also works for putting poison in bullets.

5.22 SPECIAL AMMUNITION FOR SHOTGUNS

Because of their large bore and high power, it is possible to create some extremely powerful special ammunition for use in shotguns. If a shotgun shell is opened at the top, and the shot removed, the shell can be re-closed. Then, if one can find a very smooth, lightweight wooden dowel that is close to the bore width of the shotgun, a person can make several types of shotgun- launched weapons. Insert the dowel in the barrel of the shotgun with the shell without the shot in the firing chamber. Mark the dowel about six inches away from the end of the barrel, and remove it from the barrel. Next, decide what type of explosive or incendiary device is to be used. This device can be a chemical fire bottle (sect. 3.43), a pipe bomb (sect 4.42), or a thermit bomb (sect 3.41 and 4.42). After the device is made, it must be securely attached to the dowel. When this is done, place the dowel back in the shotgun. The bomb or incendiary device should be on the end of the dowel. Make sure that the device has a long enough fuse, light the fuse, and fire the shotgun. If the projectile is not too heavy, ranges of up to 300 ft are possible. A diagram of a shotgun projectile is shown below:

```
 ____
||  |
||  |
||  | ----- bomb, securely taped to dowel
||  |
||__|
|| |
|| | ------- fuse
|| |
||
||
||
|| --------- dowel
||
||
||
||
||
|| --------- insert this end into shotgun
```

5.3 SPECIAL AMMUNITION FOR COMPRESSED AIR/GAS WEAPONS

This section deals with the manufacture of special ammunition for compressed air or compressed gas weapons, such as pump B.B guns, CO2 B.B guns, and .22 cal pellet guns. These weapons, although usually thought of as kids toys, can be made into rather dangerous weapons.

5.31 SPECIAL AMMUNITION FOR B.B GUNS

A B.B gun, for this manuscript, will be considered any type of rifle or pistol that uses compressed air or CO2 gas to fire a projectile with a caliber of .177, either B.B, or lead pellet. Such guns can have almost as high a muzzle velocity as a bullet-firing rifle. Because of the speed at which a .177 caliber projectile flies, an impact detonating projectile can easily be made that has a caliber of .177. Most ammunition for guns of greater than .22 caliber use primers to ignite the powder in the bullet. These primers can be bought at gun stores, since many people like to reload their own bullets. Such primers detonate when struck by the firing pin of a gun. They will also detonate if they are thrown at a hard surface at a great speed. Usually, they will also fit in the barrel of a .177 caliber gun. If they are inserted flat end first, they will detonate when the gun is fired at a hard surface. If such a primer is attached to a piece of thin metal tubing, such as that used in an antenna, the tube can be filled with an explosive, be sealed, and fired from a B.B gun. A diagram of such a projectile appears below:

```
  _____ primers _______
 |            |
 |            |
 |            |
 V            V
_______      _______
|__________________________ |------------------
| ****** explosive ******* |------------------ } tassel or
|__________________________ |------------------   cotton
|_____         _____|------------------
     ^
     |
     |
     |_______ antenna tubing
```

The front primer is attached to the tubing with a drop of super glue. The tubing is then filled with an explosive, and the rear primer is glued on. Finally, a tassel, or a small piece of cotton is glued to the rear primer, to insure that the projectile strikes on the front primer. The entire projectile should be about 3/4 of an inch long.

5.32 SPECIAL AMMUNITION FOR .22 CALIBER PELLET GUNS

A .22 caliber pellet gun usually is equivalent to a .22 cal rifle, at close ranges. Because of this, relatively large explosive projectiles can be adapted for use with .22 caliber air rifles. A design similar to that used in section 5.12 is suitable, since some capsules are about .22 caliber or smaller. Or, a design similar to that in section 5.31 could be used, only one would have to purchase black powder percussion caps, instead of ammunition primers, since there are percussion caps that are about .22 caliber. A #11 cap is too small, but anything larger will do nicely.

6.0 ROCKETS AND CANNONS

Rockets and cannon are generally thought of as heavy artillery. Perpetrators of violence do not usually employ such devices, because they are difficult or impossible to acquire. They are not, however, impossible to make. Any individual who can make or buy black powder or pyrodex can make such things. A terrorist with a cannon or large rocket is, indeed, something to fear.

6.1 ROCKETS

Rockets were first developed by the Chinese several hundred years before Christ. They were used for entertainment, in the form of fireworks. They were not usually used for military purposes because they were inaccurate, expensive, and unpredictable. In modern times, however, rockets are used constantly by the military, since they are cheap, reliable, and have no recoil. Perpetrators of violence, fortunately, cannot obtain military rockets, but they can make or buy rocket engines. Model rocketry is a popular hobby of the space age, and to launch a rocket, an engine is required. Estes, a subsidiary of Damon, is the leading manufacturer of model rockets and rocket engines. Their most powerful engine, the "D" engine, can develop almost 12 lbs. of thrust; enough to send a relatively large explosive charge a significant distance. Other companies, such as Centuri, produce even larger rocket engines, which develop up to 30 lbs. of thrust. These model rocket engines are quite reliable, and are designed to be fired electrically. Most model rocket engines have three basic sections. The diagram below will help explain them.

```
    _____________________________________________________________
    |____________________________________________________________| --
cardboard
     \  clay  | - - - - - - - - - - | * * * | . . . .|c|           casing
      \_______|  - - - - - - - - -  | * * * |  . . . |l|
       _______ _ - - - thrust - - -  | smoke | eject  |a|
      / clay  |  - - - - - - - - -  | * * * | . . . .|y|
     /________|______________________|_______|________|_|_______
     |______________________________________________________| --
cardboard
                                        casing
```

The clay nozzle is where the igniter is inserted. When the area labeled "thrust" is ignited, the "thrust" material, usually a large single grain of a propellant such as black powder or pyrodex, burns, forcing large volumes of hot, rapidly expanding gasses out the narrow nozzle, pushing the rocket forward. After the material has been consumed, the smoke section of the engine is ignited. It is usually a slow-burning material, similar to black powder that has had various compounds added to it to produce visible smoke, usually black, white, or yellow in color. This section exists so that the rocket will be seen when it reaches its maximum altitude, or apogee. When it is burned up, it ignites the ejection charge, labeled "eject". The ejection charge is finely powdered black powder. It burns very rapidly, exploding, in effect. The explosion of the ejection charge pushes out the parachute of the model rocket. It could also be used to ignite the fuse of a bomb...

Rocket engines have their own peculiar labeling system. Typical engine labels are: 1/4A-2T, 1/2A-3T, A8-3, B6-4, C6-7, and D12-5. The letter is an indicator of the power of an engine. "B" engines are twice as powerful as "A" engines, and "C" engines are twice as powerful as "B" engines, and so on. The number following the letter is the approximate thrust of the engine, in pounds. the final number and letter is the time delay, from the time that the thrust period of engine burn ends until the ejection charge fires; "3T" indicates a 3 second delay.

NOTE: an extremely effective rocket propellant can be made by mixing aluminum dust with ammonium perchlorate and a very small amount of iron oxide. The mixture is bound together by an epoxy.

6.11 BASIC ROCKET BOMB

A rocket bomb is simply what the name implies: a bomb that is delivered to its target by means of a rocket. Most people who would make such a device would use a model rocket engine to power the device. By cutting fins from balsa wood and gluing them to a large rocket engine, such as the Estes "C" engine, a basic rocket could be constructed. Then, by attaching a "crater maker", or CO2 cartridge bomb to the rocket, a bomb would be added. To insure that the fuse of the "crater maker" (see sect. 4.42) ignited, the clay over the ejection charge of the engine should be scraped off with a plastic tool. The fuse of the bomb should be touching the ejection charge, as shown below.

```
          _____________ rocket engine
          |                  _________ crater maker
          |                  |
          |                  |
          V                   |
     ________________________________V_
```

```
|________________________________|  _______________________
 \   | - - - - - -|***|::::|      /# # # # # # # # # # # \
  \__| - - - - - -|***|::::|  ___/  # # # # # # # # # # # \
    __  - - - - - -|***|::::|---fuse--- # #  explosive  # # )
  /  | - - - - - -|***|::::|  ___   # # # # # # # # # # # /
 /___|______________|___|____|____ \________________________/
|________________________________|
```

thrust> - - - - - -
smoke> ***
ejection charge> ::::

Duct tape is the best way to attach the crater maker to the rocket engine. Note in the diagram the absence of the clay over the ejection charge Many different types of explosive payloads can be attached to the rocket, such as a high explosive, an incendiary device, or a chemical fire bottle.

Either four or three fins must be glued to the rocket engine to insure that the rocket flies straight. The fins should look like the following diagram:

```
        |\
        | \
        |  \
        |   \  <--------- glue this to rocket engine
        |    \
        |     \
        |      \
        |      |
        |      |
        |      |
 leading edge    |
  ------->      |
        |      |
        |      |  trailing edge
        |      |    <--------
        |      |
        |      |
        |      |
        |      |
         \_____/
```

The leading edge and trailing edge should be sanded with sandpaper so that they are rounded. This will help make the rocket fly straight. A two inch long section of a plastic straw can be attached to the rocket to launch it from. A clothes hanger can be cut and made into a launch rod. The segment of a plastic straw should be glued to the rocket engine adjacent to one of the fins of the rocket. A front view of a completed rocket bomb is shown below.

```
                 |
 fin              | <------ fin
  |               |          |
  |               |          |
  |             __|__        |
  V            /     \       V
---------------|       |---------------
               \_____/
                 |o <----------- segment of plastic straw
                 |
                 |
                 | <------ fin
                 |
                 |
```

By cutting a coat hanger at the indicated arrows, and bending it, a launch rod can be made. After a fuse is inserted in the engine, the rocket is simply slid down the launch rod, which is put through the segment of plastic straw. The rocket should slide easily along a coathanger, such as the one illustated on the following page:

```
               ____
              /    \
             |      |
  cut here ______      |
             |     |
             |     |
             |    / \
             V   /   \
  _________________/     \_________________
 /                         \
/                            \
/_____________________________________________\
                    ^
                    |
                    |
        and here ______|
```

Bend wire to this shape:

```
              _______ insert into straw
              |
               |
               |
               V
    ____________________________________________
    \
     \
      \
       \
        \  <--------- bend here to adjust flight angle
         |
         |
         |
         |
         |
         | <---------- put this end in ground
         |
```

6.12 LONG RANGE ROCKET BOMB

Long range rockets can be made by using multi-stage rockets. Model rocket engines with an "0" for a time delay are designed for use in multi-stage rockets. An engine such as the D12-0 is an excellent example of such an engine. Immediately after the thrust period is over, the ejection charge explodes. If another engine is placed directly against the back of an "0" engine, the explosion of the ejection charge will send hot gasses and burning particles into the nozzle of the engine above it, and ignite the thrust section. This will push the used "0" engine off of the rocket, causing an overall loss of weight. The main advantage of a multi-stage rocket is that it loses weight as travels, and it gains velocity. A multi-stage rocket must be designed somewhat differently than a single stage rocket, since, in order for a rocket to fly straight, its center of gravity must be ahead of its center of drag. This is accomplished by adding weight to the front of the rocket, or by moving the center of drag back by putting fins on the rocket that are well behind the rocket. A diagram of a multi-stage rocket appears on the following page:

```
      ___
     /   \
     |   |
     | C |
     | M | ------ CM: Crater Maker
     |   |
     |   |
     |___|
     |   |
     |   |
     |   |
     | C | ------ C6-5 rocket engine
    /| 6 |\
   / | | | \
  /  | 5 |  \
 /   |___|   \ ---- fin
```

```
      /   /|   |\   \
     /   / |   | \   \
    /   /  |   |  \   \
   /   /   | C |   \   \
  |   /    | 6 |    \   |
  |  /     | | |     \  |
  | /      | 0 |      \ |
  |/       |___|       \|
  |       /     \       |
  \______/   ^   \______/ ------- fin
             |
             |
             |
             |
             C6-0 rocket engine
```

The fuse is put in the bottom engine.

Two, three, or even four stages can be added to a rocket bomb to give it a longer range. It is important, however, that for each additional stage, the fin area gets larger.

6.13 MULTIPLE WARHEAD ROCKET BOMBS

"M.R.V." is an acronym for Multiple Reentry Vehicle. The concept is simple: put more than one explosive warhead on a single missile. This can be done without too much difficulty by anyone who knows how to make crater-makers and can buy rocket engines. By attaching crater makers with long fuses to a rocket, it is possible that a single rocket could deliver several explosive devices to a target. Such a rocket might look like the diagram on the following page:

```
        ___
       /   \
       |   |
       | C |
       | M |
       |___|
    ___|   |___
    | |     | |
    | |  T  | |
   / \|  U  |/ \
  /   \| B |/   \
  |   || E ||   |
  | C ||   || C |
  | M ||   || M |
  |   ||___||   |
  \___/| E |\___/
       | N |
      /| G |\
      / | I | \
     /  | N |  \
    /   | E |   \
   /    |___|    \
  / fin/  |  \ fin\
 |    /   |   \    |
  \__/    |    \__/

          ^
          |____ fin
```

The crater makers are attached to the tube of rolled paper with tape. the paper tube is made by rolling and gluing a 4 inch by 8 inch piece of paper. The tube is glued to the engine, and is filled with gunpowder or black powder. Small holes are punched in it, and the fuses of the crater makers are inserted in these holes. A crater maker is glued to the open end of the tube, so that its fuse is inside the tube. A fuse is inserted in the engine, or in the bottom engine if the rocket bomb is multi stage, and the rocket is launched from the coathanger launcher, if a segment of a plastic straw has been attached to it.

6.2 CANNON

The cannon is a piece of artillery that has been in use since the 11th century. It is not unlike a musket, in that it is filled with powder, loaded, and fired. Cannons of this sort must also be cleaned after each shot, otherwise, the projectile may jam in the barrel when it is fired, causing the barrel to explode. A sociopath could build a cannon without too much trouble, if he/she had a little bit of money, and some patience.

6.21 BASIC PIPE CANNON

A simple cannon can be made from a thick pipe by almost anyone. The only difficult part is finding a pipe that is extremely smooth on its interior. This is absolutely necessary; otherwise, the projectile may jam. Copper or aluminum piping is usually smooth enough, but it must also be extremely thick to withstand the pressure developed by the expanding hot gasses in a cannon. If one uses a projectile such as a CO2 cartridge, since such a projectile can be made to explode, a pipe that is about 1.5 - 2 feet long is ideal. Such a pipe MUST have walls that are at least 1/3 to 1/2 an inch thick, and be very smooth on the interior. If possible, screw an endplug into the pipe. Otherwise, the pipe must be crimped and folded closed, without cracking or tearing the pipe. A small hole is drilled in the back of the pipe near the crimp or endplug. Then, all that need be done is fill the pipe with about two teaspoons of grade blackpowder or pyrodex, insert a fuse, pack it lightly by ramming a wad of tissue paper down the barrel, and drop in a CO2 cartridge. Brace the cannon securely against a strong structure, light the fuse, and run. If the person is lucky, he will not have overcharged the cannon, and he will not be hit by pieces of exploding barrel. Such a cannon would look like this:

```
         ___________________ fuse hole
         |
         |
         V
 ____________________________________________________________________
| |_________________________________________________________________|
|endplug|powder|t.p.| CO2 cartridge
| _______|_______|_____|____________________________________________
|_|_________________________________________________________________|
```

An exploding projectile can be made for this type of cannon with a CO2 cartridge. It is relatively simple to do. Just make a crater maker, and construct it such that the fuse projects about an inch from the end of the cartridge. Then, wrap the fuse with duct tape, covering it entirely, except for a small amount at the end. Put this in the pipe cannon without using a tissue paper packing wad. When the cannon is fired, it will ignite the end of the fuse, and shoot the CO2 cartridge. The explosive-filled cartridge will explode in about three seconds, if all goes well. Such a projectile would look like this:

```
  ___
 /   \
 |   |
 | C |
 | M |
 |   |
 |   |
 |\ /|
 | | | ---- tape
 |_|_|
   |
   | ------ fuse
```

6.22 ROCKET FIRING CANNON

A rocket firing cannon can be made exactly like a normal cannon; the only difference is the ammunition. A rocket fired from a cannon will fly further than a rocket alone, since the action of shooting it overcomes the initial inertia. A rocket that is launched when it is moving will go further than one that is launched when it is stationary. Such a rocket would resemble a normal rocket bomb, except it would have no fins. It would look like this:

```
  ___
 /   \
|     |
|  C  |
|  M  |
|     |
|     |
|_____|
|  E  |
|  N  |
|  G  |
|  I  |
|  N  |
|  E  |
|_____|
```

the fuse on such a device would, obviously, be short, but it would not be ignited until the rocket's ejection charge exploded. Thus, the delay before the ejection charge, in effect, becomes the delay before the bomb explodes. Note that no fuse need be put in the rocket; the burning powder in the cannon will ignite it, and simultaneously push the rocket out of the cannon at a high velocity.

7.0   PYROTECHNICA ERRATA

There are many other types of pyrotechnics that a perpetrator of violence might employ. Smoke bombs can be purchased in magic stores, and large military smoke bombs can be bought through adds in gun and military magazines. Also, fireworks can also be used as weapons of terror. A large aerial display rocket would cause many injuries if it were to be fired so that it landed on the ground near a crowd of people. Even the "harmless" pull-string fireworks, which consists of a sort of firecracker that explodes when the strings running through it are pulled, could be placed inside a large charge of a sensitive high explosive. Tear gas is another material that might well be useful to the sociopath, and such a material could be instantly disseminated over a large crowd by means of a rocket-bomb, with nasty effects.

7.1   SMOKE BOMBS

One type of pyrotechnic device that might be employed by a terrorist in many way would be a smoke bomb. Such a device could conceal the getaway route, or cause a diversion, or simply provide cover. Such a device, were it to produce enough smoke that smelled bad enough, could force the evacuation of a building, for example. Smoke bombs are not difficult to make. Although the military smoke bombs employ powdered white phosphorus or titanium compounds, such materials are usually unavailable to even the most well-equipped terrorist. Instead, he/she would have to make the smoke bomb for themselves.

Most homemade smoke bombs usually employ some type of base powder, such as black powder or pyrodex, to support combustion. The base material will burn well, and provide heat to cause the other materials in the device to burn, but not completely or cleanly. Table sugar, mixed with sulfur and a base material, produces large amounts of smoke. Sawdust, especially if it has a small amount of oil in it, and a base powder works well also. Other excellent smoke ingredients are small pieces of rubber, finely ground plastics, and many chemical mixtures. The material in road flares can be mixed with sugar and sulfur and a base powder produces much smoke. Most of the fuel-oxodizer mixtures, if the ratio is not correct, produce much smoke when added to a base powder. The list of possibilities goes on and on. The trick to a successful smoke bomb also lies in the container used. A plastic cylinder works well, and contributes to the smoke produced. The hole in the smoke bomb where the fuse enters must be large enough to allow the material to burn without causing an explosion. This is another plus for plastic containers, since they will melt and burn when the smoke material ignites, producing an opening large enough to prevent an explosion.

7.2 COLORED FLAMES

Colored flames can often be used as a signaling device for terrorists. by putting a ball of colored flame material in a rocket; the rocket, when the ejection charge fires, will send out a burning colored ball. The materials that produce the different colors of flames appear below.

COLOR	MATERIAL	USED IN
red	strontium salts (strontium nitrate)	road flares, red sparklers
green	barium salts (barium nitrate)	green sparklers
yellow	sodium salts (sodium nitrate)	gold sparklers
blue	powdered copper old pennies	blue sparklers,
white	powdered magnesium or aluminum	firestarters, aluminum foil
purple	potassium permanganate	purple fountains, treating sewage

7.3 TEAR GAS

A terrorist who could make tear gas or some similar compound could use it with ease against a large number of people. Tear gas is fairly complicated to make, however, and this prevents such individuals from being able to utilize its great potential for harm. One method for its preparation is shown below.

EQUIPMENT

1. ring stands (2)
2. alcohol burner
3. erlenmeyer flask, 300 ml
4. clamps (2)
5. rubber stopper
6. glass tubing
7. clamp holder
8. condenser
9. rubber tubing
10. collecting flask
11. air trap
12. beaker, 300 ml

MATERIALS

10 gms glycerine

2 gms sodium bisulfate

distilled water

1.) In an open area, wearing a gas mask, mix 10 gms of glycerine with 2 gms of sodium bisulfate in the 300 ml erlenmeyer flask.

2.) Light the alcohol burner, and gently heat the flask.

3.) The mixture will begin to bubble and froth; these bubbles are tear gas.

4.) When the mixture being heated ceases to froth and generate gas, or a brown residue becomes visible in the tube, the reaction is complete. Remove the heat source, and dispose of the heated mixture, as it is corrosive.

5.) The material that condenses in the condenser and drips into the collecting flask is tear gas. It must be capped tightly, and stored in a safe place.

7.4 FIREWORKS

While fireworks cannot really be used as an effective means of terror, they do have some value as distractions or incendiaries. There are several basic types of fireworks that can be made in the home, whether for fun, profit,
or nasty uses.

7.41 FIRECRACKERS

A simple firecracker can be made from cardboard tubing and epoxy. The instructions are below:

1) Cut a small piece of cardboard tubing from the tube you are using. "Small" means anything less than 4 times the diameter of the tube.

2) Set the section of tubing down on a piece of wax paper, and fill it with epoxy and the drying agent to a height of 3/4 the diameter of the tubing. Allow the epoxy to dry to maximum hardness, as specified on the package.

3) When it is dry, put a small hole in the middle of the tube, and insert a desired length of fuse.

4) Fill the tube with any type of flame-sensitive explosive. Flash powder, pyrodex, black powder, potassium picrate, lead azide, nitrocellulose, or any of the fast burning fuel-oxodizer mixtures will do nicely. Fill the tube almost to the top.

5) Pack the explosive tightly in the tube with a wad of tissue paper and a pencil or other suitable ramrod. Be sure to leave enough space for more epoxy.

6) Fill the remainder of the tube with the epoxy and hardener, and allow it to dry.

7) For those who wish to make spectacular firecrackers, always use flash powder, mixed with a small amount of other material for colors. By crushing the material on a sparkler, and adding it to the flash powder, the explosion will be the same color as the sparkler. By adding small chunks of sparkler material, the device will throw out colored burning sparks, of the same color as the sparkler. By adding powdered iron, orange sparks will be produced. White sparks can be produced from magnesium shavings, or from small, LIGHTLY crumpled balls of aluminum foil.

Example: Suppose I wish to make a firecracker that will explode with a red flash, and throw out white sparks. First, I would take a road flare, and finely powder the material inside it. Or, I could take a red sparkler, and finely powder it. Then, I would mix a small amount of this material with the flash powder. (NOTE: FLASH POWDER

MAY REACT WITH SOME MATERIALS THAT IT IS MIXED WITH, AND EXPLODE SPONTANEOUSLY!) I would mix it in a ratio of 9 parts flash powder to 1 part of flare or sparkler material, and add about 15 small balls of aluminum foil I would store the material in a plastic bag overnight outside of the house, to make sure that the stuff doesn't react. Then, in the morning, I would test a small amount of it, and if it was satisfactory, I would put it in the firecracker.

8) If this type of firecracker is mounted on a rocket engine, professional to semi-professional displays can be produced.

7.42 SKYROCKETS

An impressive home made skyrocket can easily be made in the home from model rocket engines. Estes engines are recommended.

1) Buy an Estes Model Rocket Engine of the desired size, remembering that the power doubles with each letter. (See sect. 6.1 for details)

2) Either buy a section of body tube for model rockets that exactly fits the engine, or make a tube from several thicknesses of paper and glue.

3) Scrape out the clay backing on the back of the engine, so that the powder is exposed. Glue the tube to the engine, so that the tube covers at least half the engine. Pour a small charge of flash powder in the tube, about 1/2 an inch.

4) By adding materials as detailed in the section on firecrackers, various types of effects can be produced.

5) By putting Jumping Jacks or bottle rockets without the stick in the tube, spectacular displays with moving fireballs or M.R.V.'s can be produced.

6) Finally, by mounting many home made firecrackers on the tube with the fuses in the tube, multiple colored bursts can be made.

7.43 ROMAN CANDLES

Roman candles are impressive to watch. They are relatively difficult to make, compared to the other types of home-made fireworks, but they are well worth the trouble.

1) Buy a 1/2 inch thick model rocket body tube, and reinforce it with several layers of paper and/or masking tape. This must

be done to prevent the tube from exploding. Cut the tube into about 10 inch lengths.

2) Put the tube on a sheet of wax paper, and seal one end with epoxy and the drying agent. About 1/2 of an inch is sufficient.

3) Put a hole in the tube just above the bottom layer of epoxy, and insert a desired length of water proof fuse. Make sure that the fuse fits tightly.

4) Pour about 1 inch of pyrodex or gunpowder down the open end of the tube.

5) Make a ball by powdering about two 6 inch sparklers of the desired color. Mix this powder with a small amount of flash powder and a small amount of pyrodex, to have a final ratio (by volume) of 60% sparkler material / 20% flash powder / 20% pyrodex. After mixing the powders well, add water, one drop at a time, and mixing continuously, until a damp paste is formed. This paste should be moldable by hand, and should retain its shape when left alone. Make a ball out of the paste that just fits into the tube. Allow the ball to dry.

6) When it is dry, drop the ball down the tube. It should slide down fairly easily. Put a small wad of tissue paper in the tube, and pack it gently against the ball with a pencil.

7) When ready to use, put the candle in a hole in the ground, pointed in a safe direction, light the fuse, and run. If the device works, a colored fireball should shoot out of the tube to a height of about 30 feet. This height can be increased by adding a slightly larger powder charge in step 4, or by using a slightly longer tube.

8) If the ball does not ignite, add slightly more pyrodex in step 5.

9) The balls made for roman candles also function very well in rockets, producing an effect of falling colored fireballs.

8.0 LISTS OF SUPPLIERS AND MORE INFORMATION

Most, if not all, of the information in this publication can be obtained through a public or university library. There are also many publications that are put out by people who want to make money by telling other people how to make explosives at home. Adds for such appear frequently in paramilitary magazines and newspapers. This list is presented to show the large number of places that information and materials can be purchased from. It also includes fireworks companies and the like.

COMPANY NAME AND A--RESS WHAT COMPANY SELLS
------------------------ ------------------

FULL AUTO CO. INC.   EXPLOSIVE RECIPES,
P.O. BOX 1881   PAPER TUBING
MURFREESBORO, TN
37133

UNLIMITED   CHEMICALS AND FUSE
BOX 1378-SN
HERMISTON, OREGON
97838

AMERICAN FIREWORKS NEWS   FIREWORKS NEWS MAGAZINE WITH
SR BOX 30   SOURCES AND TECHNIQUES
DINGMAN'S FERRY, PENNSYLVANIA
18328

BARNETT INTERNATIONAL INC.   BOWS, CROSSBOWS, ARCHERY MATERIALS,
125 RUNNELS STREET   AIR RIFLES
P.O. BOX 226
PORT HURON, MICHIGAN
48060

CROSSMAN AIR GUNS   AIR GUNS
P.O. BOX 22927
ROCHESTER, NEW YORK
14692

_
EXECUTIVE PROTECTION PRODUCTS INC.   TEAR GAS GRENADES,
316 CALIFORNIA AVE.   PROTECTION DEVICES
RENO, NEVADA
89509

BADGER FIREWORKS CO. INC.   CLASS "B" AND "C" FIREWORKS
BOX 1451
JANESVILLE, WISCONSIN
53547

NEW ENGLAND FIREWORKS CO. INC.   CLASS "C" FIREWORKS
P.O. BOX 3504
STAMFORD, CONNECTICUTT
06095

RAINBOW TRAIL   CLASS "C" FIREWORKS
BOX 581
EDGEMONT, PENNSYLVANIA
19028

STONINGTON FIREWORKS INC.   CLASS "C" AND "B" FIREWORKS
4010 NEW WILSEY BAY U.25 ROAD
RAPID RIVER, MICHIGAN
49878

WINDY CITY FIREWORKS INC.   CLASS "C" AND "B" FIREWORKS
P.O. BOX 11   (GOOD PRICES!)
ROCHESTER, INDIANNA
46975

BOOKS

THE ANARCHIST'S COOKBOOK

THE IMPROVISED MUNITIONS MANUAL

MILITARY EXPLOSIVES

FIRES AND EXPLOSIONS

9.0   CHECKLIST FOR RAIDS ON LABS

In the end, the serious terrorist would probably realize that if he/she wishes to make a truly useful explosive, he or she will have to steal the chemicals to make the explosive from a lab. A list of such chemicals in order of priority would probably resemble the following:

LIQUIDS
____

____   Nitric Acid
____   Sulfuric Acid
____   95% Ethanol
____   Toluene
____   Perchloric Acid
____   Hydrochloric Acid

SOLIDS
____

____   Potassium Perchlorate
____   Potassium Chlorate
____   Picric Acid (usually a powder)
____   Ammonium Nitrate
____   Powdered Magnesium
____   Powdered Aluminum
____   Potassium Permanganate
____   Sulfur
____   Mercury
____   Potassium Nitrate
____   Potassium Hydroxide
____   Phosphorus
____   Sodium Azide
____   Lead Acetate
____   Barium Nitrate

10.0   USEFUL PYROCHEMISTRY

In general, it is possible to make many chemicals from just a few basic ones. A list of useful chemical reactions is presented. It assumes knowledge of general chemistry; any individual who does not understand the following reactions would merely have to read the first five chapters of a high school chemistry book.

1. potassium perchlorate from perchloric acid and potassium hydroxide

   $K(OH) + HClO_4 \text{ ----> } KClO_4 + H_2O$

2. potassium nitrate from nitric acid and potassium hydroxide

   $\text{"} + HNO_3 \text{ ----> } KNO_3 + \text{"}$

3. ammonium perchlorate from perchloric acid and ammonium hydroxide

   $NH_3OH + HClO_4 \text{ ----> } NH_3ClO_4 + \text{"}$

4. ammonium nitrate from nitric acid and ammonium hydroxide

   $NH_3OH + HNO_3 \text{ ----> } NH_3NO_3 + \text{"}$

5. powdered aluminum from acids, aluminum foil, and magnesium

A. $\text{aluminum foil} + 6HCl \text{ ----> } 2AlCl_3 + 3H_2$

B. $2AlCl_3 \text{ (aq)} + 3Mg \text{ ----> } 3MgCl_2 \text{ (aq)} + 2Al$

The Al will be a very fine silvery powder at the bottom of the container which must be filtered and dried. This same method works with nitric and sulfuric acids, but these acids are too valuable in the production of high explosives to use for such a purpose, unless they are available in great excess.

/----------------------------\

House Hold equivalants

----- ---- -----------

Name	Equivalant
acetic acid	vinegar
aluminum oxide	alumia
aluminum potassium sulfate	alum
aluminum sulfate	alum
ammonium hydroxide	ammonia

carbon carbonate	chalk
carbon tetrachloride	cleaning fluid
calcium hypochloride	bleaching powder
calcium oxide	lime
calcium sulfate	plaster of paris
carbonic acid	seltzer
ethylene dichloride	dutch fluid
ferric oxide	iron rust
glucose	corn syrup
graphite	pencil lead
hydrochloric acid	muriatic acid
hydrogen peroxide	peroxide
lead acetate	sugar of lead
lead tetrooxide	red lead
magesium silicate	talc
magesium sulfate	Epsom salts
naphthalene	mothballs
phenol	carbolic acid
potassium bicarbonate	cream of tarter
potassium chromium sulfate	chrome alum
potassium nitrate	saltpeter
sodium dioxide	sand
sodium bicarbonate	baking soda
sodium borate	borax
sodium carbonate	washing soda
sodium choride	salt
sodium hydroxide	lye
sodium silicate	water glass
sodium sulfate	glaubers' salt
sodium thiosulfate	photographers hypo
sulferic acid	battery acid
sucrose	cane sugar
zinc choride	tinner's fluid
------------	--------------

-=] Smoke Bomb [=-
--- ----- ---- ---

Mix:
4 parts sugar
- ----- -----
6 parts potassium nitrate

Heat:
over low flame till melts. stir well, then pour into container. Before it solidifies, put a few matches in for fuses.

*One pound of this stuff will fill a block nicely with a thick cloud of white smoke.
--- ----- ------

-=] Generic bomb [=-
--- ------- ---- ---

1) Aquire a glass container

2) Put in a few drops of gasoline
3) Cap the top
4) Now turn the container around to coat the inner surfaces and then evaporates
5) Add a few drops of potassium permanganate (<-Get this from a snakebite kit)
6) The bomb is detonated by throwing aganist a solid object.

AFTER THROWING THIS THING RUN
LIKE HELL THIS THING PACKS
ABOUT 1/2 STICK OF DYNAMITE

(> EXPLOSIVE INFO
==============

WHEN PETROLEUM JELLY AND POTASSIUM CHLORATE ARE MIXED IN A ONE TO ONE RATIO BY WEIGHT, IT MAKES A TOTALY SAFE WET COMPOUND BUT WHEN DRIED IT BECOMES HIGHLY EXPLOSIVE AND SHOCK SENSITIVE.

MIX 3 GRAMS OF POTASSIUM IODIDE AND 5 GRAMS OF IODINE IN A BEAKER WITH 50 ML OF WATER. THEN ADD 20 ML OF AMMONIUM HYDROXIDE [AMMONIA WATER 10%]. FILTER THIS SUBSTANCE AND THE RESULTING SOLID IS CALLED NITROGEN TRIIODIDE. WHEN THIS IS WET IT IS SAFE, BUT WHEN DRY BECOMES VERY EXPLOSIVE AND SHOCK SENSITIVE.

(TO SET OFF ABOVE EXPLOSIVES, PUT THE MIXTURE ON OR IN SOMETHING THEN DROP IT SORT OF LIKE AN IMPACT BOMB. IT, LIKE A HAND GRENADE, WILL EXPLODE ON CONTACT WITH ANOTHER OBJECT.)

OTHER UNLAWFULS
Written by: The Hoe Hopper
Distributed by The Blue Buccaneer
[> Call the EXODUS AE Line <]

Carbide Bomb

This is EXTREMELY DANGEROUS. Exercise extreme caution....

Obtain some calcium carbide. This is the stuff that is used in carbide lamps and can be found at nearly any hardware store. Take a few pieces of this stuff (it looks like gravel) and put it in a glass jar with some water. Put a lid on tightly. The carbide will react with the water to produce acedylene carbonate which is similar to the gas used in cutting torches. Eventually the glass with explode from internal pressure. If you leave a burning rag nearby, you will get a nice fireball!

Portable Grenade Launcher

If you have a bow, this one is for you. Remove the ferrule from an aluminum arrow, and fill the arrow with black powder (I use grade FFFF, it burns easy) and then glue a shotshell primer into the hole left where the ferrule went. Next, glue a BB on the primer, and you are ready to go!

Make sure no one is nearby. Little shreds of aluminim go everywhere.

Auto Exhaust Flame Thrower

For this one, all you need is a car, a sparkplug, ignition wire and a switch. Install the spark plug into the last four or five inches of the tailpipe by drilling a hole that the plug can screw into easily.

Attach the wire (this is regular insulated wire) to one side of the switch and to the spark plug. The other side of the switch is attached to the positive terminal on the battery.

With the car running, simply hit the switch and watch the flames fly!!! Again be careful that no one is behind you! I have seen some of these flames go 20 feet!!!

[HOME EXPLOSIVES]

->UNSTABLE EXPLOSIVE<-
^^^^^^^^^^^^^^^^^^^^^^^

1) MIX SOLID NITRIC IODINE WITH HOUSE-HOLD AMMONIA.

2) WAIT OVERNIGHT

3) POUR OFF LIQUID

4) DRY MUD ON BOTTOM TO HARD (LIKE CON-CRETE)

5) THROW SOMETHING AT IT!

6) CAUTION: MERE FRICTION MAY SET THIS OFF!
....

->SMOKE BOMB<-
^^^^^^^^^^^^^^^

```
1) MIX:     3 PARTS SUGAR
          ----------------------
           6 PARTS EPSON SALTS
```

2) PUT IN A TIN CAN, AND ONTO A LOW FLAME (LIKE A LIGHTER)

3) LET GEL & HARDEN

4) PUT MATCH IN AS A FUSE.

5) LIGHT AND RUN LIKE HELL 'CAUSE 4
POUNDS WILL FILL A CITY BLOCK...

....

->MEDIUM EXPLOSIVE<-
^^^^^^^^^^^^^^^^^^^^^

```
1) MIX:    7 PARTS POTASSIUM CHLORATE
          --------------------------
               1 PART VASELINE
```

2) TO IGNITE, USE AN ELECTRIC CHARGE OR
A LONG FUSE.

....

->CAR BOMB<-
^^^^^^^^^^^^^

1) PUT LIQUID DRANO INTO A PILLBOX (THE
KIND YOU GET WHEN YOU'RE ON A PRE-
SCRIPTION, NOTHING ELSE WILL WORK)

2) CLOSE LID & POP THE THING INTO THE GAS
TANK

3) RUN

....

->PLASTIC EXPLOSIVE<-
^^^^^^^^^^^^^^^^^^^^^^

```
1)MIX:       2 PARTS VASELINE
           ------------------
            1 PART GASOLINE
```

2) IGNITE WITH AN ELECTRIC CHARGE

3)   THIS WILL THROW FLAMING GASOLINE GEL

(How To Make Mercury Fulminate))

When employing the use of any high explosive,an individual must also use some kind of detonating device.Blasting caps are probably the most popular today,since they are very functional and relativly stable.The prime ingrediant in most blasting caps and de tonating devices in general is mercury fulminate.There are several methods for preparing mercury fulminate.

Method No.1 for the preparation of
Mercury Fulminate:

1. Take 5 grams of pure mercury and mix is with 35 ml. of nitric acid.

2.The mixture is slowly and gentle heated.As soon as the solution bubbles and turns green, one knows that the silver mercury is dissolved.

3. After it is dissolved, the solution should be poured,slowly,into a small flask of ethyl alcohol.This will result in red fumes.

4. After a half hour or so,the red fumes will turn white, indicating that the process is nearing its final stage.

5. after a few minutes, add distilled water to the solution.

6. The entire solution is now filtered, in order to obtain the small white crystals.These crystals are pure mercury fulminate,but should be washed many times, and tested with litmus paper for any remaining undersiable acid.

Method No. 2 for the preparation of
Mercury Fulminate:

1. Mix one part mercuric oxide with ten parts ammonia solution.When ratios are described,they are always done according to weight rather than volume.

2. After waiting eight to ten days,one will see that the mercuric oxide has reacted with the ammonia solution to produce the white fulminate crystals.

3. These crystals must be handled in the same way as the first method described, in that they must be washed many times and given several litmus paper tests.

Many other fulminates can be made in the same manner as above,but i will not go into these,since most are extremely unstable and sensitive to shock.All fulminates including mercury fulminate,are sensitive to shock and friction,and in no circumstances should they be handled in a rough or careless manner..

*   THE MEYTHAL HYDRATE   *
*   CANNON   *

Ingredients Needed:
1) A Metal Tube measuring about 4-5 inches in diameter
2) Meythal Hydrate (Local Hardware, Paint Section) $1.99
3) Cap for one end of the Metal Tube

4) A Drill
5) Some Matches
6) Some Tennis Balls

Procedure:

Get the Metal Tube, and cut it so it is about 3 feet long, then jam the cap onto the end of the Metal Tube, and make sure you have a tight fit, because you don't want the thing to blow off! Next, drill a small hole, big enough for a match, at the base of the Metal Tube, just above where the cap rim is.

One, Two, Three CANNON!

*- Make sure the cap is tight, or else.....?

To Fire:

Here is the easy part, the cannon can be used as a mortar, or a bazooka, it depends on the target. Now, get a capful of the Meythal Hydrate and pour it into the metal tube, get a tennis ball and ram it down the tube, make sure the tennis ball is tight, and doesn't just fall down, or it won't work. Pick your target and light a match and stick it in the hole, the gas vapourizes and THUD goes the tennis ball. An easier method of lighting, if you don't want to be in the vicinity, is a piece of fuse, which anybody can buy at Robinson's Guns, it is in the counter to the right of the cash register, on the top shelf.

Diagram:

```
      -----------------------------------------------\
                                            () Ý
      ------------------------------------------------/
                                          ^
                                          Ý Drill Hole Here
```

Military Explosives
Part One

Definitions

Military Demolition:

Military demolition is the destruction by fire, water, explosive, mechanical, or other means of area structures, facilities, or materials to accomplish a military objective. Demolitions are explosives used for such purposes. Demolitions have offensive and defensive uses. Examples are the removal of enemy barriers to facilitate the advance and the construction of friendly barriers to delay or restrict enemy movement.

Explosives:

Explosives are substances that, through chemical reaction, violently change to a gaseous form. In doing so, they release pressure and heat equally in all directions. They are classified as low or high according to the detonating velocity or speed (in meters or feet per second) at which this change takes place and other characteristics such as their shattering effect.

Low Explosives:

Low explosives change from a solid to a gaseous state slowly aver a sustained period (up to 400 meters or 1,300 feet per second). This characteristic makes low explosives ideal when a pushing or shoving effect is required. Examples of low explosives are smokeless and black powders.

High Explosives:
High explosives change to a gaseous state almost instantaneously at 1,000 meters per second (3,280 feet per second) to 8,500 meters per second (27,888 feet per second), producing a shattering effect on the target. Use high explosives when a shattering effect, or brisance, is required.

Relative Effectives (RE) Factor:
Explosives vary in detonating rate or velocity (meters or feet per second), as well as other characteristics, such as density and energy production. These characteristics determine their effectiveness for cutting, breaching, or cratering charges. Most military demolitions involve cutting or breaching. The amount of explosive used is adjusted by a relative effectiveness (RE) factor, which is based upon the shattering effect of the explosive in relation to that of trinitrotoluene (TNT). The shattering effect of a high explosive is related to its detonating velocity. For example, TNT with a detonating velocity of 6,900 meters per second has a relative effectiveness factor of 1.00, while Composition C4 with a detonating velocity of 8,040 meters per second has a relative effectiveness factor of 1.34.

Cratering Effect:
The cratering effect of high explosives depends upon their total energy content, which determines the amount of energy available to throw the broken material from the crater. Because a shattering effect is not required to form a crater, low-velocity explosives are generally more effective for cratering purposes. Therefore, the relative effectiveness factor is not considered in determining the effect of a cratering charge. Blasting road craters or ditches normally requires large amounts of explosives. Because it is effective and inexpensive, an ammonium nitrate-based cratering charge is used as a standard cratering charge.

Characteristics

To be suitable for use in military operations, explosives must have certain properties. Military explosives must -- Be inexpensive to manufacture and capable of being produced from readily available raw material.
Be relatively insensitive to shock or friction, yet able to positively detonate by easily prepared initiators. Have the shattering effect and potential energy adequate for the purpose. Be stable enough to retain usefulness for a reasonable time when stored in any climate at temperatures between -80 and +165 degrees Fahrenheit. Have high density (weight per unit of volume).
Be suitable for use under water or in damp climates.
Have minimum toxicity (poisonous effects) when stored, handled, and detonated.
Be a convenient size and shape for packaging, storing, distributing, handling, and emplacing by troops.
Have high energy output per unit of volume.

Detonation

The detonation or burning of all explosives produces poisonous fumes.
The chemicals used in explosives are poisonous.
Caution personnel against inhaling fumes or ingesting explosives.
When explosives are used in closed areas or underground, allow adequate time for the fumes to dissipate before investigation. Control the explosives to prevent their use, such as burning as a source of heat or cooking, for other than intended purpose.

Fire Hazards

Explosives contain their own oxidizer. Burning explosives cannot be extinguished by smothering or with water. In fact, smothering will probably cause and explosion. Because of the possibility of detonation while explosives are burning, observe the minimum safe distance. WARNING: Personnel should not attempt to extinguish burning explosives without expert advice and assistance.

Fire Safety Precautions for Transport

If fire breaks out in a vehicle transporting explosives, try to stop the vehicle away form any populated buildings. Stop traffic in both directions, and warn drivers, passengers, and occupants of nearby buildings to keep at least 2,000 feet away. Inform police and firefighting authorities that the cargo is explosives. If a fire involves only the engine, cab, chassis, or tires, make an effort to put out the fire with fire extinguishers, sand, dirt, or water. If the fire spreads to the body or cargo, STOP FIGHTING THE FIRE AND EVACUATE THE AREA to a distance of at least 2,000 feet.

: Kitchen Chemistry

n order to spare yourself some problems....Time Delays:------------ These delays only work with the 2nd and 3rd variations: Coat the solid inVaseline, or in the case of Idea#2, coat the top of the ingredient in the filmcontainer with a liquid soap. This slows down the reaction.A (Not 5-6) Rule on Xplosives:----------------------------- Treat all explosives like a pressure sensitive H-Bomb. There will be notrouble if you do.Formula #1---------- Crystal Drano and gasoline react violently... I think that this would be a good one for idea #1 and idea #2. In idea #1 place the gasoline in the container, and place the crystal Drano in the pipe... In idea #2 place the Drano in the 36 mm film container. and th gas in the jar. I would put a delay on this one.Formula #2---------- This one is probably only good for idea#1, and it is extremely dangerous. Inthis case, you need to get Calcium Carbide at a Hardware store (Calcium C. lamps use it) Place the C.C. in the pipe. Place the water in the jar, and wrap a

wrag soaked in gasoline around it. When ready to use, simply light therag, and break the jar... GET RID OF IT THEN!!! DANGEROUSER than the others, as the expanding gas blows the pipe apart, then gas is lit, and it explodes.Formula #3---------- This is an oldy, but goody, and the materials are beyond easy to get. Thematerials are: Baking Soda and Vinegar. This one works for all three ideas,and is especially good for three, since it won't explode, just foam up because of the hole in the top. It never hurts to be safe, so play with the am'ts... In idea#1 place the vinegar in the jar the same in #2. In #3, placethe vinegar in the can.Formula #4---------- This one uses Granulated pool Chlorine and PineSol. If it is not in a closedcontainer, a gout of flame will fire up. If in a container, an explosion results because of pressure. Very much like Formula #1. Play with it in idea#3. Place the solid in the paper towels and use small am'ts first.Thermite:--------- Thermite, is a mixture, of 25% aluminum filings

, 75% iron oxide filings.When lit, by something like black powder, (I.E. Thermite core) it burns FIERCELY. Recquires a fairly high temperature to start.Napalm------ The BEST formula for Napalm is gasoline and styrofoam. Let it dissolve, andspoon out xs gasoline.Smoke Mixture------------- This is mixture that burns fiercely, when fresh and low when not, but in anycase it gives off a dense white smoke. It is composed of Potassium Nitrate andSugar in a ratio of 6 parts p.n. to 4 parts sugar. Mix this all together, thenheat over a low flame. It will slowly form a thick brown syrupy mixture. Whenstill in a liquid form, pour it into a mold. When still syrupy, it burns witha hot flame about 1 foot high. Smoke Mixture #2---------------- This is a mixture of 6 parts charcoal, 3 parts potassium nitrate, and 1 partsulfur. Mix well... It is very much like black powder, but smokes more, andstinks to the point of driving people away. Less heavy on the potassium nitrate than the other.Nut Busters----------- The

se are easy to make, and may be altered in power easily. Take a shotgunshell, determine the gauge yourself, but start with a 20 gauge. Tape a largemarble to the primer. You may, or may not want to remove the shot. I would STRONGLY suggest it. All you do then is throw it. The weight of the marble pulls it down, hits the primer, and puff. Don't forget to be behind something if you leave the shot in.SODA BOMBS---------- Ingredients: Granulated Pool Chlorine (At least 75% Calcium Hypochlorite) - Sugar - Water - 2 Liter Soda Bottle Take a quarter of Chlorine and place it in an empty and dry 2 literbottle. Put the same amount of sugar and place it in the bottle too. Addenough water to make the mixture soapy. Put the cap on and throw it away!!!It splatters a noxious and blinding chemical when it goes off. As the sugarand chlorine dissolve in the water, they will react with each other. The Bombis as loud as an M-80. The bomb will take anywhere from 30 seconds to 5minutes to go off. So if it doesn't e

xplode, still stay a way and come backthe next day and examine it. If it doesn't work, try adjusting the amounts ofsugar and chlorine. ** I didn't write this one, but thanx to whoever did **Black Powder------------Composition: 74% Potassium Nitrate(Saltpeter) 15.6% Charcoal 10.4% Sulfur Grind this all together, until you have a fine powder. Put in a container andmix until it is nearly black. Add some rubbing alcohol and mix together some more. Use your imagaination on ways to mix it, just don't get it too hot.Black powder is used for a lot of things, including blasting, so don't forgetabout black powder, just because you want to make C-4!!! The ingredients maybe obtained at a drug store. ** Note: Make sure you grind the Charcoal into a very fine powder!!! **Amidpulver---------- Amidpulver is a flahless, almost smokeless powder. (When fired from a gun. It goes easier on the potassium nitrate than black powder, although it absorbswater from the air, and this deactivates it. Store in a waterproofed conta

inerCompositions: Amid #1 Amid #2Potassium Nitrate: 40% 14%Ammonium Nitrate: 38% 37%Charcoal 22% 49%Of the two, #2 is the better formula.Ammonium Nitrate is a fertilizer, and can be obtained at a feed store.+------------------------------------++ Call these TOXIC boards: ++ The Mob 313-782-9519 ++ D.A.][313-271-1095 ++ D.A. Main 313-386-5469 ++ The Hole in the Wall 313-383-4996++ Marble Madness 619-353-0970 ++------------------------------

------+(C) January 1987, Milamber.Thanx to Tigger for distribution. I may be found at any of the above boards, for questions and comments.Disclaimer:----------- The above is intended for informational uses only. (Right?) And the writeris NOT responsible for ANY injuries incurred. Please work with small quantities to get the feel. Keep about 100-300 feet away, until you have hadexpedon't know why I put my name here, some scum will remove it, I'm sure.]
Downloaded from P-80 Systems......

NAPALM GRENADE

Napalm is in itself a very simple substance...it can be used for many things...Here's what'cha need:

```
Gasoline                              Joy or Palmolive(I prefer Joy)
A Coke can with a sawed off top       Ammonia Pellets
A Drill                               Some bendable wire
A Nail
```

First,make a mixture of 1/2 Joy(my favorite),and 1/2 Gasoline.
Take the coke can, and fill it half full with this mixture...
it should look like this:

```
      -^-^-^-^-^-^-^-
      !           !
      !           ! <-Coke Can
      !           !
      !=============!
      !=============!
      !=============! <-Mixture
      !=============!
      ---------------
```

Now,take the drill(or some sharp object)and put a hole through the ammonia pellet big enough for the nail.. Put the nail through the pellet(which I might add can be picked up at any farm supply store)and wire that to the top of the can so the nail can be slipped out easily,allowing the pellet to drop...WARNING: DO NOT LET THAT PELLET FALL INTO THE MIXTURE,AS YOUR WIFE WILL SOON BECOME A WIDOW!! Wait until you are ready to set it off to let it drop...It should look like this:

```
    (=======<+>=========)
    ! ^^Nail  ^^Pellet   !
    !                  !
    !                  !
    !                  !
    !====================!
    !====================! <-Mixture
    !====================!
    !====================!
    ----------------------
```

And there is your Napalm grenade...

NOTE: IF YOU SCREW UP, BE AWARE THAT NAPALM STICKS TO SKIN WHILE IT BURNS

-\ Explosives and Bombs /- :

-\ Firebombs /-

Most fire bombs are simply gasoline filled bottles with a fuel soaked rag in the mouth (the bottle's mouth, not yours). The original Molotov cocktail, and still about the best, was a mixture of one part gasoline and one part motor oil. The oil helps it to cling to what it splatters on.

Some use one part roofing tar and one part gasoline. Fire bombs have been found whcih were made by pouring melted wax into gasoline.

=======================================

-\ Napalm /-

About the best fire bomb is napalm. It has a thick consistancy, like jam and is best for use on vehicles or buildings.

Napalm is simply one part gasoline and one part soap. The soap is either soap flakes or shredded bar soap. Detergents won't do.

The gasoline must be heated in order for the soap to melt. The usual way is with a double boiler where the top part has at least a two-quart capicity. The water in the bottom part is brought to a boil and the double boiler is taken from the stove and carried to where there is no flame.

Then one part, by volume, of gasoline is put in the top part and allowed to heat as much as it will and the soap is added and the mess is stirred until it thickens. A better way to heat gasoline is to fill a bathtub with water as hot as you can get it. It will hold its heat longer and permit a much larger container than will the double boiler.

==

-\ Match Head Bomb /-

Simple safety match heads in a pipe, capped at both ends, make a devestating bomb. It is set off with a regular fuse

A plastic Baggie is put into the pipe before the heads go in to prevent detonation by contact with the metal.

Cutting enough match heads to fill the pipe can be tedious work for one.

==

-\ Fuse Ignition Fire Bomb /-

A four strand homemade fuse is used for this. It burns like fury. It is held down and concealed by a strip of bent tin cut from a can. The exposed end of the fuse is dipped into the flare igniter. To use this one, you light the fuse and hold the fire bomb until the fuse has burned out of sight under the tin. Then throw it and when it breaks, the burning fuse will ignite the contents.

-\ Disclaimer /-

I am not responsible for any death or injury caused by using what is contained herin.

MAKING POCKET ROCKETS

WHAT IS A POCKET ROCKET ?

A DEVICE MEASURING APPROXIMATELY 1 3/4 INCHES LONG, THAT WHEN PROPERLY MADE WILL FLY 4-8 FEET, IF PROPERLY SET OFF.

ALTHOUGH NOT A POWERFUL DEVICE, IT IS
WELL SUITED TO ANNOYING YOUR DORM-MATE,
OR PERHAPS A CLASSMATE DURING THOSE
OFTEN RECURRING SESSIONS OF BOREDOM.

MATERIALS NEEDED

1-PACKET OF MATCHES (CARDBOARD MATCHES,
  NOT WOODEN ONES)
1-PIN (A SMALL ONE, STEAL IT FROM MOMS
  SEWING BASKET)
1-PIECE OF ALUMINUM FOIL, 1 SQUARE
  INCH FOR EVERY ROCKET (REYNOLDS WRAP)
1-PAIR OF SCISSORS (OPTIONAL)
1-PAPER CLIP (OPTIONAL)
1-CIGARETTEE LIGHTER (OPTIONAL)

MAKING THE LITTLE BUGGERS

OKAY SO YOU'VE RAIDED THE HOUSE FOR ALL
THE STUFF....
1) TAKE THE PACK OF MATCHES APART BY
   REMOVING THE LITTLE STAPLE AT THE
   BOTTOM.
2) USE THE SCISORS TO CUT OFF A SINGLE
   MATCH FROM THE BUNCH.
3) CUT OUT A 1 INCH SQUARE OF ALUMINUM
   FOIL AND FOLD IT IN HALF.
4) PUT THE HEAD OF THE MATCH IN THE
   CENTER OF THE CREASE AND PRESS THE
   FOIL SO IT FORMS AROUND THE HEAD
5) WRAP THE REST OF THE FOIL AROUND THE
   MATCH HEAD AS TIGHTLY AND NEATLY AS
   POSSIBLE.

NOW U HAVE A MATCH WITH THE HEAD
WRAPPED UP IN FOIL, WITH THE FOIL
COMING 1/2 INCH DOWN FROM THE HEAD.
THIS IS THE WAY YOU'D STORE THEM IF YOU
WEREN'T GOING TO FIRE THEM IMMEDIATELY.

NOTE - NEATNESS COUNTS, TIGHTNESS
COUNTS, YES YOU CAN JUST RIP A MATCH
OUT, AND RIP FOIL, BUT THE END RESULT
WON'T WORK AS WELL.

PREPARATION FOR LAUNCH
----

1) TAKE THE PIN AND PUSH IT UNDER THE
   FOIL UNTIL YOU FEEL THE POINT START
   TO CRUSH THE HEAD. KEEP THE PIN AS
   CLOSE TO THE MATCH AS POSSIBLE WHEN

DOING THIS.

2) BEND THE PAPER CLIP TO FORM A 45 DEG ANGLE WITH THE HORIZON, AND SET IT ON A RELATIVELY NON-FLAMMABLE SURFACE, POINTING IN THE DIRECTION YOU WISH TO FIRE THE ROCKET.

3) REMOVE THE PIN FROM THE MATCH AND GINGERLY SET THE MATCH ON THE PAPER CLIP, BEING CAREFUL NOT TO CRUSH THE FOIL DOWN (THE PLACE THE PIN WAS IS NOW THE EXHAUST PORT).

LAUNCH

HEAT THE HEAD OF THE MATCH (THE PART COVERED WITH FOIL) TILL IGNITION.

NOTES

NEATNESS ALWAYS COUNTS ON THESE BUGGERS , ALWAYS USE SCISSORS WHEN POSSIBLE. YOU SHOULD USE A LIGHTER INSTEAD OF A MATCH SO U DONT GET SCORCHED FINGERS. I HAVE YET TO GET A 2 STAGE ROCKET TO FLY, IF YOU DO UPDATE THE FILE. IF ALL OF THIS IS TOO COMPLICATED FOR YOU THEN PERHAPS PAGE 45 OF 'THE GREAT INTERNATIONAL PAPER AIRPLANE BOOK' SAID IT BETTER...

"POCKET ROCKET. INSTRUCTIONS: WRAP ALUMINUM FOIL AROUND UPPER HALF OF PAPER MATCH. PUSH STRAIGHT PIN UP UNDER FOIL TO HEAD OF MATCH AND REMOVE AGAIN LEAVING EXHAUST CHANNEL. PLACE MATCH ON OPENED PAPER CLIP AND HOLD LIGHTED MATCH TO TIP. STEP BACK."

COUNTERINTELLIGENCE CHALLENGES IN A CHANGING WORLD

In recent years, the world witnessed some truly amazing events--the fall of the Berlin Wall and the reunification of East and West Germany, the beginnings of democratic governments across Eastern Europe, and the easing of political tensions between the United States and the Soviet Union. As a result, the current perception of most Americans is that foreign intelligence activity directed against the United States and the West is decreasing, and therefore, the need for an active, aggressive counterintelligence response has abated. Unfortunately, this is far from true.

There can be no doubt that important changes are taking place in the world today. However, improved diplomatic relations do not necessarily decrease the foreign intelligence threat to U.S. national security. The truth remains: That threat still exists, as it did in the past and as it will in the future.

DECADE OF THE 1980S

The last decade of the cold war, the 1980s, was designated by the media as "The Decade of the Spy." It was a time when Americans knew who their enemies were--a time when President Ronald Reagan referred to the Soviet Union as "The Evil Empire." The American public showed strong support of counterintelligence efforts and participated in the process by reporting suspicious events.

During the 1980s, more than 45 people were arrested for espionage. Increased human and technical resources, enhanced analytical and training programs, and improved coordination within the U.S. intelligence community and with friendly foreign intelligence services contributed significantly to these arrests. However, much of the success in counterintelligence efforts came as a result of a heightened public awareness of the full damage caused by espionage, as well as the public's support of the measures designed to protect Americas vital information.

In addition to the importance of public awareness, the 1980s taught us several other important lessons. First, the American public received a rude awakening regarding the vulnerability of the U.S. national security community from spies within its own ranks. For example, both John Walker and Jerry Whitworth served in the U.S. Navy; Karel Koecher, Larry Chin, and Edward Howard all worked for the Central Intelligence Agency (CIA); Ronald Pelton was a National Security Agency employee; Richard Miller was an FBI Special Agent.

Second, many of the dangers were posed by volunteers. That is, many of those arrested during the 1980s, including Walker, simply offered to spy on their country. And they offered to spy not because they had ideological differences with the U.S. Government or ideological sympathy with a foreign government, as was the case during World War II and the first decade of the Cold War. They spied for the basest of reasons--money.

Third, prosecuting spies was found to be an effective tool to determine the extent of the damage caused to national security. Unfortunately, some of the espionage cases of the

1980s resulted in grave damage to U.S. national security interests. But, without the prosecutions that followed, an accurate accounting of what was lost would not have been possible, and appropriate steps to minimize the damage would not have been taken. Fortunately, in 45 percent of the espionage cases during the 1980s, the work the U.S. counterintelligence community uncovered either prevented the espionage activity or significantly limited the damages.

THE CHANGING WORLD

In the 1990s, with the easing of tensions between superpowers and military blocs, it is no longer possible to identify the U.S. counterintelligence mission in terms of these relationships alone--the world has become much too complex for that. America has negotiated historic arms reduction treaties with the Soviets. The Soviets have introduced their programs of Glasnost, openness to the West, and Perestroika, internal economic and political restructuring. And, the world has witnessed the nations of Eastern Europe revolt against their former Communist leaders in favor of new freedom and economic diversity, and in some cases, more democratic forms of government.

While all Americans can agree that the world has changed, and most see that change as positive in terms of an enhanced prospect for world peace, the public tends to view this new world order to be devoid of danger. So, the logic goes, that if there is no longer a threat to U.S. national security, then counterintelligence measures are not needed.

But, the reality is that arms reduction treaties between the United States and the Soviet Union give Soviet "inspectors" potential access to some of this country's most sensitive projects. Glasnost has dramatically expanded the number of exchanges between the United States and the Soviet Union in such areas as business, science, and education. In fact, since Glasnost, the number of Soviets traveling to the United States increased almost 400 percent; in 1990 alone, more than 100,000 Soviets visited the United States. Past experience shows that these exchange groups often contain intelligence officers. Furthermore, the countries of Eastern Europe, while attempting to move away from the Soviet sphere of influence, are now fighting for their own economic survival--and they, too, have a need for Western technology.

CURRENT INTELLIGENCE THREATS

Arms control treaties between the Soviet Union and the United States will hopefully lead to a diminished threat level between the nations. However, from a counterintelligence perspective, these treaties will give the Soviet intelligence services routine access to sensitive areas and to knowledgeable Americans who are linked to classified information which, until now, was attainable only on a very limited basis. Other treaties presently being negotiated, concerning strategic arms reduction and chemical weapons, would require numerous verification sites, again expanding Soviet access.

But, the Soviets are interested in more than American military secrets. The Soviet economy is in desperate shape and can be revitalized with Western technology, capital, and expertise. In order to strengthen that economy, the chairman of the KGB has publicly stated that it plans to assist Soviet businesses because, as he says, "They are not good businessmen." The Soviets have systematically expanded their intelligence collection beyond military intelligence targets and now routinely include Western economic information and technologies.

Since the Soviets can no longer rely on their former surrogate intelligence services in the Eastern Bloc to collect intelligence for them, they must find other sources of intelligence and develop new surrogate services. The Soviets have started using the intelligence services of other countries to obtain Stealth technology and acquire restricted computer technologies for themselves.

Recent repression by the Soviet government of dissent in the Baltic Republics may very well signal a new shift in Soviet internal policy away from the liberalization of Glasnost. This, in turn, may have far-reaching implications involving the Soviet military and its intelligence services, U.S. national security, and the emerging "new world order."

All in all, while the nature of the Soviet intelligence threat may be changing, its objectives and actions are not. The Soviet intelligence services are more active now than they have been at any time in the past 10 years, and there is every reason to believe that they will continue their pursuit of Western intelligence during the 1990s.

The threat of Eastern European countries to the United States cannot be fully assessed because they themselves have not yet fully defined the nature and scope of their intelligence services. Some of these countries are no longer collecting intelligence on behalf of the Soviet Union; however, they will, in all likelihood, refocus their collection activities in the United States to fulfill their own requirements. Since, as with the Soviets, the current major focus of these nations is economic reorganization and growth, they also have a real need for Western technology.

What about the People's Republic of China (PRC)? The PRC has the largest foreign official presence in the United States--2,700 diplomats and commercial officials, 43,000 scholars, 25,000 commercial delegates visiting the United States annually, and 20,000 emigres coming to America each year. The PRC remains a major counterintelligence threat to the United States. Their intelligence services target well-educated Chinese-American scientists and other professionals who have access to useful information and technology using the approach: "Please help China modernize."

While the Soviet Union, the former Eastern Bloc countries, and the People's Republic of China are all traditional intelligence threats, U.S. counterintelligence efforts can no longer focus exclusively on these countries. In this information age, any number of countries can attempt to establish the infrastructure required to carry out intelligence collection activities in the United States, both overtly and clandestinely. Essentially, Americans need to be concerned about nontraditional intelligence threats to this country as well.

With this point in mind, the intelligence activities of countries in the Middle East and Central Asia are becoming more significant. For example, the Iraqi intelligence service was very active in the United States during the 1980s, and in light of the recent war in the Persian Gulf, its activities are likely to continue.

COUNTERINTELLIGENCE RESPONSIBILITIES

The FBI is charged with countering the hostile activities of foreign intelligence services in the United States by identifying and neutralizing these activities. It does this by penetrating these services, disrupting or publicizing their illegal activities, and expelling, arresting, or prosecuting those responsible.

However, the FBI cannot meet its counterintelligence mission alone. Coordination of counterintelligence operations with other members of the intelligence community, and frequently joint operations, is critical to the Bureau's success, along with the support of the Executive and Legislative Branches of the Federal Government, the law enforcement community, and the American public.

While the FBI has the responsibility to make the public more aware of the hostile intelligence threat, it relies heavily on information from the public to fulfill its counterintelligence mission. Because many Americans no longer perceive the Soviet Union and other Eastern European countries as a threat to U.S. security, the FBI must comprehensively expose the full scope of this threat to American institutions, facilities, and citizens. The purpose behind this is to protect national security, not to discourage improved relations and trade between the United States and the rest of the world.

CONCLUSION

The world is in a constant state of flux. What is true today may not be true tomorrow. For this reason, it is critical to identify the exact nature of any hostile intelligence threat to national security and to counter that threat.

A heightened awareness by all Americans is the most effective weapon available to accomplish this task. By working together, citizens and law enforcement agencies can successfully meet the counterintelligence challenges of today and those of the years to come.

ESPIONAGE AWARENESS PROGRAMS

On a Saturday morning in January 1980, while on patrol, Cpl. Thomas E. Hutchins, a Maryland State trooper, noticed a car with diplomatic tags traveling slowly on a major highway. The trooper also observed that the driver of the car was constantly checking his rearview mirror as he drove. The actions of the driver, combined with the speed of the vehicle, the early hour, and the diplomatic tags, aroused his suspicions enough that he ran a check of the car's registration. It was registered to a Soviet, Ivan Ivanovich Odintsov. The trooper then asked himself what could a Soviet diplomat be doing at 6:00 a.m. on a cold Saturday morning? Now, more suspicious than ever, Corporal Hutchins continued to follow the diplomat's car.

The diplomat, noticing the patrol vehicle, tried to evade the trooper. Then, he attempted several countersurveillance techniques to determine if he was still being followed. Losing his composure, the diplomat accelerated to more than 60 m.p.h. and ran a stop sign. This was when Corporal Hutchins decided to pull him over.

As he approached the stopped vehicle, Corporal Hutchins noticed that the Soviet diplomat appeared frightened and nervous. When asked to identify himself, Odintsov stated he was a Soviet diplomat and produced a diplomatic passport and a District of Columbia driver's license. Also, with no prompting, he told the officer that he was going fishing.

Corporal Hutchins, seeing no fishing gear in the car and knowing that there was no place to fish in the area, asked his dispatcher to contact the U.S. State Department to advise them of the stop and seek its guidance. A short time later, the dispatcher informed the trooper that no one was available at the State Department at that hour. Concerned about the proximity of the Soviet to Andrews Air Force Base and the Naval Communications Station, which were both less than 5 miles away, but running out of alternatives, he decided to issue the Soviet a warning citation and allowed him to depart. However, before the end of his patrol, the trooper did notify the Security Police at the airbase of the Soviet's presence in the area.

Unknown to Corporal Hutchins, the Soviet was a known KGB intelligence officer. Later, in 1985, the FBI learned that Odintsov was one of the KGB officers responsible for handling John Walker, the most notable Soviet penetration of the U.S. Navy in this century. The fact that Walker was not identified on that Saturday morning, 5 years earlier, was just bad luck.

COUNTERINTELLIGENCE MISSION

Identifying agents and activities of foreign intelligence services in the United States is the most difficult task of counterintelligence. Without identification, plans cannot be developed to penetrate and neutralize an espionage operation. However, once the identification is made, even the most sophisticated network can be brought down.

To be successful in its counterintelligence mission, the FBI depends on an informed, enlightened citizenry and local and State law enforcement to assist in the identification process. Public participation in the identification process has led to the identification of past KGB activities, and it still remains critical to current counterintelligence efforts.

Unfortunately, however, the American public's perception of the Soviet threat has changed considerably in recent years. In June 1989, public opinion polls conducted in the United States indicated that 65% of Americans no longer consider the Soviet Union an immediate threat. (1) And, Stern Magazine reported that during the summer of 1989, 50% of West Germans polled believed they were more threatened by the United States than the Soviet Union. (2) Interesting facts, especially since both polls were taken before the fall of the Berlin Wall.

Now, incidents witnessed by American citizens that were previously viewed as suspicious or threatening are no longer seen in that light. In turn, citizens report fewer of these incidents.

Today, the uninformed might conclude that an effective counterintelligence program is no longer necessary. Nothing could be further from the truth. As Nicholas Daniloff, former Moscow reporter for U.S. News and World Report and one-time prisoner of the KGB, stated in a recent newspaper article, "Despite the reforms...Soviet spying against the United States will continue with intensity for a long time to come." (3)

What the American public fails to realize is that the Soviets continue to spend billions of dollars annually on espionage and intelligence collections activities in an attempt to close the gap with the West in microelectronics, computers, and sophisticated weapons systems. (4) In fact, heightened citizen awareness and cooperation is needed just as much now as it was in the past.

THE DECA PROGRAM

The FBI has developed a variety of techniques and programs to counter the activities of hostile foreign intelligence services in the United States. One of the most effective of these efforts is the Development of Espionage and Counterintelligence Awareness Program (DECA). DECA links the FBI's counterintelligence program to the security countermeasures employed by defense contractors. Under this program, FBI resources are focused on the spy's targets--U.S. employees with access to classified information--not on the intelligence officer or the diplomatic establishment.

The DECA Program operates in all 56 FBI Field Offices. In each office, a DECA coordinator administers the program. The coordinator's primary responsibility is to visit firms that have been awarded classified contracts to update them on current foreign intelligence threats.

Because of the dramatic increase in the threat posed by foreign intelligence services, the focus of the DECA Program has been expanded to now include American firms not engaged in classified government contracts and the public in general. Also, with the increase in exchange programs among Soviet and East European governments and U.S. Government agencies and local law enforcement agencies, DECA coordinators are now providing espionage briefings to other Federal agencies and local police departments.

At the beginning of 1990, the FBI appointed a national DECA coordinator (NDC) to manage the program throughout the country. A short time later, a national DECA advisory committee was organized. This committee, composed of DECA coordinators from the larger FBI field offices, assists the NDC with the formulation and implementation of DECA goals, training, slides, videos, (5) and literature.

INDUSTRIAL SECURITY AWARENESS COUNCIL

In August 1988, as another step designed to increase espionage awareness, the Industrial Security Awareness Council (ISAC) was formed. ISAC is a joint Government/private sector working group whose membership includes the Defense Investigative Service (DIS), the FBI, and 11 defense contractors. (6)

ISAC's goal is to promote security awareness in the defense industry by focusing on the collective resources of industry and government. Its members share awareness resources, thereby reducing needless duplication of efforts that occur when companies operate alone, without coordination and cooperation. This concept has since been expanded by DIS and the FBI to other regions of the country and plans are in progress to make it a national organization.

CONCLUSION

The United States continues to have secrets that some foreign powers seek and are willing to steal. These secrets go beyond the strategic military and technological information that impact on national security. They also include sensitive economic information and proprietary technologies of America's private sector. These technologies may never be classified, but their loss could have a negative impact on those companies who developed them. A loss in the private sector, if significant enough to threaten a company's survival, could also endanger national security.

The successes achieved by Soviet and other foreign intelligence services during the 1980s serve to reinforce the fact that counterintelligence is a strategic issue that requires a coordinated, effective national response. Because the world is so complex and is in a constant state of flux, the FBI must be able to articulate clearly this evolving intelligence threat and work with America's private sector to meet today's counterintelligence challenges successfully.

FOOTNOTES

[1] David Remnick, The Washington Post, June 13, 1989, p. A 1.

[2] Ibid.

[3] Nicholas Daniloff, "Reforms In Soviet Union Only Increase Appetites For Secrets From The West," Los Angeles Times, August 9, 1989.

[4] Hughes Aircraft Company, A Counterintelligence Awareness Primer, 1987, p. 5.

[5] Hughes Aircraft Company and the FBI jointly produced a video entitled "Espionage 2000." This 30-minute video contains interviews of experts in the counterintelligence and security countermeasures fields discussing important awareness issues. It is available to any government agency or defense contractor for use in espionage awareness programs by contacting the FBI, the Defense Investigative Service, or the Hughes Aircraft Company.

[6] The 11 defense contractors are Aerospace Corporation, Hughes Aircraft Company, Jet Propulsion Laboratory, Lockheed Aeronautical Systems Company, Logicon, McDonnell Douglas Corporation, Northrop Corporation, Rockwell International Corporation, Science Applications International, Trident Data Corporation, and TRW.

EFFECTIVE CROWD CONTROL

While small to midsized departments may be located in areas where the problem of crowd control is virtually nonexistent, there could be times when they have to police large groups of people during special local events. There are also times when smaller cities that border large municipalities must deal with the overflow of people attending an event in that municipality.

For example, Covington, Kentucky, currently has 91 sworn officers to police a population of 50,000. But, because Covington is separated from Cincinnati, Ohio, by only the Ohio River, the Covington Police Department must prepare for overflow crowds that are generated by special events held in Cincinnati. And, because police managers must regard even peaceful crowds as having riot potential, planning is critical to effective crowd control. (1) This article discusses exactly what areas of concern should be addressed when planning for crowd control and how police managers should approach the task.

PLANNING FOR CROWD CONTROL

A step-by-step plan is important to effective crowd control. In order to ensure a well-policed event, police managers should prepare ahead of time for any conceivable problems.

Personnel

To plan for effective crowd control, police managers should consider what personnel resources are available. For example, a traffic division with officers who are experienced in traffic flow is invaluable. Also invaluable when planning for crowd control is a police auxiliary, which could help in areas where sworn officers are not needed. In extreme cases, the National Guard can be used as additional resources.

Other personnel resources to draw from include officers from neighboring police departments, the fire department, the public works department, the Red Cross, and citizen band radio clubs. Private businesses, such as bus companies, are also sometimes willing to lend equipment to assist in crowd control. Buses make effective barricades to block intersections.

Advance Notification

Another important task when planning for a special event is to notify businesses and residents in the affected area of how much disruption they can expect. Ground rules should be discussed ahead of time so that there are no misunderstandings during the event. Also, if public transportation is expected to be disrupted, alternate routes should be designated prior to the event, and fire and ambulance personnel should be contacted to determine checkpoints for rapid access routes.

Traffic Control

Traffic control is important to policing any major event. "No parking" areas should be designated and posted before the event. Officials should advertise these restrictions through the media and through flyers sent to residents and businesses in the affected areas.

Officials should also contract with a wrecker service to tow vehicles parked in restricted areas. Because special events often place unusual demands on wrecker services, they should be given advance notice of what to expect. It is also important to choose an impoundment location and agree on the release procedure.

Command Posts

Command posts are an integral part of any special events operation. Department personnel should determine how much space they need for the post, the amount of parking space available in the areas being considered, and whether the locations have land lines for communication purposes. Officials should also make provisions for a remote dispatch location. If officers have more than one channel on their radios, this could be as simple as switching to a secondary channel for the event and using a portable radio with a charger.

If an event lasts more than 8 hours, food, coffee, and soft drinks should be available in the command post for officers who work the detail. Police managers should also make arrangements to clean the post after use, especially if the space was loaned to the department by a local business.

Assignments

All officers who work the event should receive clear, written instructions about the assignment. For example, a map of the event area should be prepared, showing its parameters, with all checkpoints clearly marked. If a specific checkpoint is one of "no-access under any circumstance," the officer assigned to that checkpoint should be aware of that stipulation ahead of time.

Officials should also prepare a contingency personnel plan in the event officers who are assigned to work the event call in sick. And, there should be additional flexibility in the assignments in order to cover holes in the perimeters that even the most careful planner may overlook.

Also a consideration when planning for personnel is whether a meal break will be necessary for the officers. Although extra teams are sometimes required to relieve officers, if enough officers are assigned to the teams, half the team can be relieved at a time.

Equipment

Extra equipment should always be available during large events. Police managers should ensure that extra radios, flashlights, batteries, and handcuffs are stored at the command post. When planning for extra equipment, police managers should also consider whether there will be special transportation needs. All-terrain vehicles (ATV) and golf carts that local businesses may loan to the department could prove invaluable. Officers can use ATVs to check unpaved areas and police managers can use golf carts to get to checkpoints if the size of the crowd does not permit using an automobile.

Special Considerations

Officials should make every effort to keep large events free of alcohol. If this is impossible, either through legal means or simple reasoning, managers should document problems arising from the use of alcohol to argue for alcohol-free events in the future.

If officials are successful in banning alcohol consumption during the event, it is important to publicize this fact. All coolers taken into the event area should be checked for alcohol, and dumpsters should be available at the perimeters to dispose of any confiscated liquor.

The Perimeter

Police managers should decide ahead of time what the perimeter of the event site will be and then publicize this perimeter. Officials should bear in mind that if the perimeter is too large, it will be difficult to control the crowd, and the officers would have too large an area to police. The perimeter should be checked thoroughly for any gaps that would allow lapses in security. Specific areas should be blocked, including intersections and checkpoints.

It may also be prudent to block off parking lots inside the perimeter. If a large amount of pedestrian traffic is expected following the event, the mixture of automobiles and pedestrians could prove dangerous. Controlling the parking lots allows the bulk of the pedestrian traffic to leave the perimeter first. Cars can then leave in stages, minimizing the likelihood of either a pedestrian/automobile accident or total gridlock.

THE EVENT

Before

Except for the officers who need to start their shift earlier in order to remove cars parked in restricted areas or to block off critical areas, officers working the detail should assemble about 1 hour before the event. During this time, police managers can hold a final briefing with the supervisors and discuss any necessary changes. They can also ensure that all officers are using the correct radio channel and give directions for ending the detail.

Just prior to the start of the event, officers should again check the restricted area for possible problems. It is much easier to resolve problems before the crowds begin to arrive than to deal with both problems and crowds.

During

The majority of the officers should position themselves at the perimeter of the event. By keeping the majority of the officers where the spectators pass, the perceived numbers advantage remains with the police. It also makes it easier for police managers to know the location of their officers. And, although most of the officers involved in controlling the crowd will be on foot, mobile units should also be available to respond to critical incidents that occur within or around the perimeter.

The number of officers working together in a group will vary with the situation, but no officers should work alone. Also, if possible, officers from a plainclothes unit should mingle with the crowd. Not only can plainclothes officers spot violations more easily than uniformed officers, but they also can make quick arrests that minimize any disruptions to the crowd.

Any person arrested during the event should be quickly removed from the crowd and transported away from the area by officers who are specifically assigned this duty. This minimizes the loss of personnel who are working the actual event.

When the event ends, stragglers sometimes remain. To counter this problem, floodlights that can be borrowed from the local fire department should be concentrated on the areas in which spectators are likely to congregate. This serves as a signal that it is time to leave. Officers should also scan the area for any remaining spectators as they leave their posts to return to the command post.

After

The hours following the end of an event are busy for patrol officers. If possible, officials should schedule additional patrol units to work until things return to normal. Because no major event can be kept completely alcohol and drug free, patrol units may have to deal with fights, injuries, and accidents that occur among the spectators. (2)

All officers should report to the command post before going off duty. This allows officials to record overtime and check the records for accuracy, as well as recover any equipment that has been loaned out.

Police managers should keep detailed records of the planning stages, and they should compile a list of recommended changes for policing the next event. They should also write formal letters of appreciation to any person outside the department who donated equipment or assisted in some other manner.

CONCLUSION

Policing an event that generates large crowds is a major undertaking that requires extensive planning. Police managers must follow a step-by-step plan that ensures that the crowd is controlled with the fewest number of problems possible. A well-developed, well-executed plan results in events that are safe to police officers, visitors, and the community.

FOOTNOTES

(1) Richard A. Berk, "Collective Behavior" (Dubuque, Iowa: William C. Brown Co., 1974).

(2) Adrian F. Aveni, "The Not-So-Lonely Crowd: Friendship Groups in Collective Behavior," Sociometry, vol. 40, No. 1, January 1977, pp. 96-99.

CUSTODIAL INTERROGATION:

In Minnick v. Mississippi, (1) the U.S. Supreme Court announced a rule of law that could have a substantial impact on the way many law enforcement agencies conduct custodial interrogations. Specifically, the Court severely curtailed the law enforcement officer's ability to reinitiate custodial interrogation of suspects who had previously invoked the right to counsel.

This article examines the Minnick decision and assesses its impact. It also suggests legitimate steps officers can take to limit its adverse effects on criminal investigations.

SUMMARY OF FACTS

Robert Minnick and James "Monkey" Dyess escaped from the Clarke County Jail in Mississippi and were in the process of burglarizing a mobile home when they were surprised by the arrival of the occupants. Using weapons found in the home, the escapees murdered two of the occupants and eventually fled the scene in a stolen pickup truck. Minnick was arrested 4 months later in California on a fugitive warrant.

Following his arrest, Minnick was interviewed by two FBI agents. Prior to this interview, he was advised of his Miranda (2) rights, and although he refused to sign a waiver, he agreed to answer some questions. (3) During the course of the interview, Minnick made some incriminating statements before telling the agents that he would make a more-complete statement when his lawyer was present. Believing that Minnick had invoked his right to counsel, the agents promptly terminated the interview.

Following the FBI interview, Minnick met with appointed counsel. Three days later, Deputy Sheriff J.C. Denham of Clarke County, Mississippi, arrived in California and attempted to interview Minnick. Although once again declining to sign a written waiver of his Miranda rights, Minnick agreed to talk with Denham. Statements made during the subsequent interview ultimately led to Minnick's prosecution for murder.

Prior to trial, Minnick moved to suppress his statements made to Denham. That motion was denied by the trial court, and Minnick was sentenced to death after being found guilty on two counts of capital murder. Minnick's conviction and sentence were upheld on appeal by the Mississippi Supreme Court. (4) However, on review, (5) the U.S. Supreme Court reversed the conviction.

THE COURT'S ANALYSIS

The fifth amendment to the U.S. Constitution provides in part that "no person...shall be compelled in any criminal case to be a witness against himself...." (6) Over 2 decades ago, the Supreme Court in Miranda v. Arizona (7) held that custodial interrogation of an individual creates a psychologically compelling atmosphere that works against this fifth amendment protection. (8)

In other words, the Court in Miranda presumed that an individual in custody undergoing police interrogation would feel compelled to respond to police questioning. This compulsion, which is a by-product of most custodial interrogations, (9) directly conflicts with an individual's fifth amendment protection against self-incrimination. Accordingly, the Court developed the now-familiar Miranda warnings as a means of reducing the compulsion attendant in custodial interrogations.

The Miranda rule requires that these warnings be given and the embodied rights waived prior to the initiation of custodial interrogations.

If Miranda warnings are given, and individuals in custody choose to exercise their rights by invoking either the right to silence or counsel, the Court has held that all interrogations must cease immediately. (10) Whether, and under what conditions, law enforcement officers may subsequently readvise an individual of his rights and attempt to secure a waiver depends on which rights the individual has invoked.

In Michigan v. Mosley, (11) the Supreme Court essentially interpreted the invocation of the right to silence as a request for time so a suspect could think clearly about the situation. If the suspect's initial request is scrupulously honored, the Court held that attempts to reinterrogate may occur if given the time asked for, or if he indicates, by initiating communications, that he had enough time to think and has changed his mind.

As a result, reinterrogations following an invocation of the right to silence are deemed appropriate if: 1) A reasonable period of time has elapsed; (12) or 2) interrogation was initiated by the suspect. In either case, any renewed attempts to interrogate a suspect must be preceded by a fresh warning of Miranda rights and a waiver of those rights.

An invocation of the right to counsel, on the other hand, necessarily carries with it a different set of procedural safeguards. Obviously, a suspect invoking the right to counsel is not simply asking for time to assess the situation; he is, instead, requesting the assistance of an attorney. Whether this request is satisfied by giving the suspect an opportunity to consult with an attorney or requires the actual presence of an attorney during questioning was the issue before the Court in Minnick.

Minnick's motion to suppress the statements made to Denham was based on his claim that under the fifth amendment, (13) the earlier invocation of his right to counsel during the FBI interview precluded Denham from making any subsequent attempts to question him in the absence of counsel. In opposition, the government argued that Minnick's fifth amendment rights had been satisfied when he was given the opportunity to consult with his counsel on two or three occasions prior to meeting with Denham. In order to resolve this issue, the Supreme Court found it necessary to revisit the Miranda decision and its progeny to determine when, if ever, law enforcement officers may reinitiate interrogation of an in-custody suspect who has invoked the right to counsel.

"MIRANDA" REVISITED

In Miranda, the Court held that "once an individual in custody invokes his right to counsel, interrogation `must cease until an attorney is present; at that point, the individual must have an opportunity to confer with the attorney and to have him present during any subsequent questioning."' (14) Later, in Edwards v. Arizona, (15) the Supreme Court attempted to clarify its holding in Miranda by announcing the following rule:

> "...an accused..., having expressed his desire to deal with police only through counsel, is not subject to further interrogation by the authorities until counsel has been made available to him, unless the accused himself initiates further communication, exchanges, or conversations with the police." (16)

Following Edwards, many courts focused on the expression "made available to him" and concluded that the rule simply required that a suspect in custody who had invoked the right to counsel be given the opportunity to consult or confer with his attorney before law enforcement officers could lawfully attempt to reinterrogate him. (17) Under this interpretation, there would be no necessity to show that the suspect had actually consulted with an attorney, but only that he had been afforded the opportunity to do so. The Supreme Court, however, held that such an interpretation of Edwards was both unintended and inconsistent with Miranda. Therefore, the Court concluded that "when counsel is requested [by a suspect in custody], interrogation must cease, and officials may not reinitiate interrogation without counsel present, whether or not the accused has consulted with his attorney." (18) Applying this rule to the facts in Minnick, the Court found that because Minnick had invoked his right to counsel during the FBI interview and Deputy Sheriff Denham subsequently reinitiated interrogation without counsel being present, Minnick's rights under Miranda had been violated, and the resulting statements must be suppressed.

IMPACT OF "MINNICK"

As a result of Minnick, law enforcement officers will be unable to interrogate a suspect in custody once that suspect has invoked the right to counsel unless: 1) The suspect's attorney is actually present; or 2) the suspect changes his mind and reinitiates the interrogation. (19) Because the first alternative is frequently unpalatable and the second unlikely, custodial reinterrogations after requests for counsel may quickly become rare.

Although not specifically addressed by the Supreme Court, it is important to note that the rule in Minnick will undoubtedly apply regardless of the crime that is the intended topic of the reinterrogation. (20) In other words, when an individual is advised of his Miranda rights and invokes the right to counsel, he is not simply saying that he will not deal with the police about the crime for which he has been arrested without the assistance of an attorney. Rather, a request for counsel under these conditions implies that the individual will not deal with the police on any criminal matter without the benefit of counsel. Consequently, once a suspect invokes the right to counsel under the fifth amendment, law enforcement officers are prohibited from initiating further custodial interrogation involving the original crime or any other criminal act without complying with the dictates of Minnick by having the suspect's attorney present.

Moreover, the rule in Minnick appears to be perpetual; once a suspect in custody invokes the right to counsel, the prohibition against reinterrogation remains in effect as long as custody continues. Conceivably, a suspect who invokes the right to counsel during the early stages of custody and is thereafter unable to make bond could be shielded from all further interrogation throughout the remainder of the prosecution of the case and for as long as he is incarcerated. (21)

LIMITING THE ADVERSE EFFECTS OF "MINNICK"

Writing the dissenting opinion in Minnick, Justice Scalia recognized the far-reaching effects of the Court's decision on law enforcement when he made the following statement:

> "Today's ruling, that the invocation of a right to counsel permanently prevents a police-initiated waiver, makes it largely impossible for the police to urge a prisoner who has initially declined to confess to change his mind--or indeed, even to ask whether he has changed his mind." (22)

While the Minnick decision may hamper law enforcement efforts to conduct custodial interrogations, there are certain legitimate steps law enforcement officers can take to limit its adverse effects on criminal investigations.

The first step law enforcement officers should take is to ensure that they understand and take advantage of the procedural differences that are required when a suspect invokes the right to silence as opposed to invoking the right to counsel. Because there is a significant difference between the procedural protections offered to a suspect who invokes the right to counsel and one who merely expresses a desire to remain silent, law enforcement officers should be certain they know which right a suspect is invoking. If, following the advice of rights, the suspect's response leads officers to believe that the suspect is invoking his rights, but the officers are unsure of which right is being invoked, the officers could conceivably follow up by asking the suspect if he is, in fact, invoking the right to silence. If a suspect gives an affirmative response, then officers should immediately stop questioning. However, since only the right to silence has been invoked, a second attempt to obtain a waiver may be made

SEE NOTES AT END FOR INFO ON SOURCES OF THESE DOCUMENTS

CENTRAL INTELLIGENCE AGENCY
WASHINGTON 25, D. C.

OFFICE OF THE DIRECTOR 25 APR 1956

MEMORANDUM FOR: The Honorable J. Edgar Hoover
Director, Federal Bureau of Investigation

SUBJECT : Brainwashing

The attached study on brainwashing was prepared by my staff in response to the increasing acute interest in the subject throughout the intelligence and security components of the Government. I feel you will find it well worth your personal attention. It represents the thinking of leading psychologists, psychiatrists and intelligence specialists, based in turn on interviews with many individuals who have had personal experience with Communist brainwashing, and on extensive research and testing. While individuals specialists hold divergent views on various aspects of this most complex subject, I believe the study reflects a synthesis of majority expert opinion. I will, of course, appreciate any comments on it that you or your staff may have.

(signed)
Allen W. Dulles
Director

ENCLOSURE

OA 53-37

A REPORT ON COMMUNIST BRAINWASHING

The report that follows is a condensation of a study by training experts of the important classified and unclassified information available on this subject.

BACKGROUND

Brainwashing, as a technique, has been used for centuries and is no mystery to psychologists. In this sense, brainwashing means involuntary re-education of basic beliefs and values. All people are being re-educated continually. New information changes one's beliefs. Everyone has experienced to some degree the conflict that ensues when new information is not consistent with prior belief. The experience of the brainwashed individual differs in that the inconsistent information is forced upon the individual under controlled conditions after the possibility of critical judgment has been removed by a variety of methods.

There is no question that an individual can be broken psychologically by captors with knowledge and willingness to persist in techniques aimed at deliberately destroying the integration of a personality. Although it is probable that everyone reduced to such a confused, disoriented state will respond to the introduction of new beliefs, this cannot be stated dogmatically.

PRINCIPLES OF HUMAN CONTROL AND REACTION TO CONTROL

There are progressive steps in exercising control over an individual and changing his behaviour and personality integration. The following five steps are typical of behaviour changes in any controlled individual:

1. Making the individual aware of control is the first stage in changing his behaviour. A small child is made aware of the physical and psychological control of his parents and quickly recognizes that an overwhelming force must be reckoned with. So, a controlled adult comes to recognize the overwhelming powers of the state and the impersonal, "incarcerative" machinery in which he is enmeshed. The in -dividual recognizes that definite limits have been put upon the ways he can respond.

(Approved for Release) (62-80750-2712X)
(Date: 8 FEB 1984)

2. Realization of his complete dependence upon the controlling system is a major factor in the controlling of his behavior.The controlled adult is forced to accept the fact that food, tobacco,praise, and the only social contact that he will get come from the very interrogator who exercises control over him.

----

3. The awareness of control and recognition of dependence result in causing internal conflict and breakdown of previous patterns of behaviour. Although this transition can be relatively mild in the case of a child, it is almost invariably severe for the adult

undergoing brainwashing. Only an individual who holds his values lightly can change them easily. Since the brainwasher-interrogators aim to have the individuals undergo profound emotional change, they force their victims to seek out painfully what is desired by the controlling individual. During this period the victim is likely to have a mental breakdown characterized by delusions and hallucinations.

4. Discovery that there is an acceptable solution to his problem is the first stage of reducing the individual's conflict. It is characteristically reported by victims of brainwashing that this discovery led to an overwhelming feeling of relief that the horror of internal conflict would cease and that perhaps they would not, after all, be driven insane. It is at this point that they are prepared to make major changes in their value-system. This is an automatic rather than voluntary choice. They have lost their ability to be critical.

5. Reintergration of values and identification with the controlling system is the final stage in changing the behaviour of the controlled individual. A child who has learned a new, socially desirable behaviour demonstrates its importance by attempting to asapt the new behaviour to a variety of other situations. Similar states in the brainwashed adult are

(SECTION DELETED BY CIA)

pitiful. His new value-system, his manner of perceiving,organizing,and giving meaning to events, is virtually independent of his former value-system.He is no longer capable of thinking or speaking in concepts other than those he has adopted. He tends to identify by expressing thanks to his captors for helping him see the light.Brainwashing can be achieved without using illegal means.Anyone willing to use known principles of control and reactions to control and capable of demonstrating the patience needed in raising a child can probably achieve successful brainwashing.

COMMUNIST CONTROL TECHNIQUES AND THEIR EFFECTS

A description of usual communist control techniques follows.

1. Interrogation. There are at least two ways in which "interrogation" is used:

a. Elicitation, which is designed to get the individual to surrender protected information, is a form of interrogation. One major difference between elicitation and interrogation used to achieve brainwashing is that the mind of the individual must be kept clear to permit coherent, undistorted disclosure of protected information.

b. Elicitation for the purpose of brainwashing consists of questioning,argument,indoctrination,threats,cajolery,praise,hostility, and a variety of other pressures. The aim of this interrogation is to hasten the breakdown of the individual's value system and to encourage the substitution of a different value-system. The procurement of protected information is secondary and is used as a device to increase pressure upon the individual. The term "interrogation" in this paper will refer, in general, to this type. The "interrogator" is the individual who conducts this type of interrogation and who controls the administration of the other pressures. He is the protagonist against whom the victim develops his conflict, and upon whom the victim develops a state of dependency as he seeks some solution to his conflict.

2. Physical Torture and Threats of Torture. Two types of physical torture are distinguishable more by their psychological effect in inducing conflict than by the degree of painfulness:

a. The first type is one in which the victim has a passive role in the pain inflicted on him (e.g.,beatings). His conflict involves the decision of whether or not to give in to demands in order to avoid further pain. Generally, brutality of this type was not found to achieve the desired results. Threats of torture were found more effective, as fear of pain causes greater conflict within the individual than does pain itself.

b. The second type of torture is represented by requiring the individual to stand in one spot for several hours or assume some other pain-inducing position. Such a requirement often engenders in the individual a determination to "stick it out." This internal act of resistance

----

provide a feeling of moral superiority at first. As time passes and his pain mounts,however, the individual becomes aware that it is his own original determination to resist that is causing the continuance of pain. A conflict develops within the individual between his moral determination and his desire to collapse and discontinue the pain. It is this extra internal conflict, in addition to the conflict over whether or not to give in to the demands made of him, that tends to make this method of torture more effective in the breakdown of the individual personality.

3. Isolation. Individual differences in reaction to isolation are probably greater than to any other method. Some individuals appear to be able to withstand prolonged periods of isolation without deleterious effects, while a relatively short period of isolation reduces others to the verge of psychosis. Reaction varies with the conditions of the isolation cell. Some sources have indicated a strong reaction to filth and vermin, although they had negligible reactions to the isolation. Others reacted violently to isolation in relatively clean cells. The predominant cause of breakdown in such situations is a lack of sensory stimulation (i.e.,grayness of walls,lack of sound,absence of social contact,etc.). Experimental subjects exposed to this condition have reported vivid hal-

licinations and overwhelming fears of losing their sanity.

4. Control of Communication. This is one of the most effective methods for creating a sense of helplessness and despair. This measure might well be considered the cornerstone of the communist system of control. It consists of strict regulation of the mail,reading materials, broadcast materials, and social contact available to the individual. The need to communicate is so great that when the usual channels are blocked, the individual will resort to any open channel, almost regardless of the implications of using that particular channel. Many POWs in Korea, whose only act of "collaboration" was to sign petitions and "peace appeals," defended their actions on the ground that this was the only method of letting the outside world know they were still alive. May stated that their morale and fortitude would have been increased immeasurably had leaflets of encouragement been dropped to them. When the only contact with the outside world is via the interrogator, the prisoner comes to develop extreme dependency on his interrogator and hence loses another prop to his morale.

Another wrinkle in communication control is the informer system. The recruitment of informers in POW camps discouraged communication

between inmates.POWs who feared that every act or thought of resistance would be communicated to the camp administrators, lost faith in their fellow man and were forced to "untrusting individualism." Informers are also under several stages of brainwashing and elicitation to develop and maintain control over the victims.

5. Induction of Fatigue. This is a well-known device for breaking will power and critical powers of judgment. Deprivation of sleep results in more intense psychological debilitation than does any other method of engendering fatigue. The communists vary their methods. "Conveyor belt" interrogation that last 50-60 hours will make almost any individual compromise, but there is danger that this will kill the victim. It is safer to conduct interrogations of 8-10 hours at night while forcing the prisoner to remain awake during the day. Additional interruptions in the remaining 2-3 hours of allotted sleep quickly reduce the most resilient individual . Alternate administration of drug stimulants and depressants hastens the process of fatigue and sharpens the psychological reactions of excitement and depression.

Fatigue, in addition to reducing the will to resist,also produces irritation and fear that arise from increased "slips of the tongue." forgetfulness, and decreased ability to maintain orderly thought processes.

6. Control of Food,Water and Tobacco. The controlled individual is made intensely aware of his dependence upon his interrogator for the

quality and quantity of his food and tobacco. The exercise of this control usually follows a pattern. No food and little or no water is permitted the individual for several days prior to interrogation.When the prisoner first complains of this to the interrogator, the latter expresses surprise at such inhumane treatment. He makes a demand of the prisoner. If the latter complies,he receives a good meal. If he does not, he gets a diet of unappetizing food containing limited vitamins,minerals, and calories. This diet is supplemented occasionally by the interrogator if the prisoner "cooperates." Studies of controlled starvation indicate that the whole value-system of the subjects underwent a change. Their irritation increased as their ability to think clearly decreased. The control of tobacco presented an even greater source of conflict for heavy smokers. Because tobacco is not necessary to life, being manipulated by his craving for it can in the individual a strong sense of guilt.

7. Criticism and Self-Criticism. There are mechanisms of communist thought control. Self-criticism gains its effectiveness from the fact that although it is not a crime for a man to be wrong, it is a major crime to be stubborn and to refuse to learn. Many individuals feel intensely relieved in being able to share their sense of guilt. Those individuals however, who have adjusted to handling their guilt internally have difficulty adapting to criticism and self-criticism. In brainwashing ,after a sufficient sense of guilt has been created in the individual, sharing and self-criticism permit relief. The price paid for this relief, however, is loss of individuality and increased dependency.

8. Hypnosis and Drugs as Controls. There is no reliable evidence that the communists are making widespread use of drugs or hypnosis in brainwashing or elicitation. The exception to this is the use of common stimulants or depressants in inducing fatigue and "mood swings."

9. Other methods of control, which when used in conjunction with the basic processes, hasten the deterioration of prisoners' sense of values and resistance are:

a. Requiring a case history or autobiography of the prisoner provides a mine of information for the interrogator in establishing and "documenting" accusations.

b. Friendliness of the interrogator , when least expected, upsets the prisoner's ability to maintain a critical attitude.

c. Petty demands, such as severely limiting the allotted time for use of toilet facilities or requiring the POW to kill hundreds of flies, are harassment methods.

d. Prisoners are often humiliated by refusing them the use of toilet facilities during interrogator until they soil themselves. often prisoners were not permitted to bathe for weeks until they felt contemptible.

e. Conviction as a war criminal appears to be a potent factor in creating despair in the individual. One official analysis of the pressures exerted by the ChiComs on "confessors" and "non-confessors" to participation in bacteriological warfare in Korea showed that actual trial and conviction of "war crimes" was overwhelmingly associated with breakdown and confession.

f. Attempted elicitation of protected information at various times during the brainwashing process diverted the individual from awareness of the deterioration of his value-system. The fact that, in most cases, the ChiComs did not want or need such intelligence was not known to the prisoner. His attempts to protect such information was made at the expense of hastening his own breakdown.

THE EXERCISE OF CONTROL: A "SCHEDULE" FOR BRAINWASHING

From the many fragmentary accounts reviewed, the following appears to be the most likely description of what occurs during brainwashing .

In the period immediately following capture, the captors are faced with the problem of deciding on best ways of exploitation of the prisoners. Therefore, early treatment is similar both for those who are to be exploited through elicitation and those who are to undergo brainwashing. concurrently with being interrogated and required to write a detailed personal history, the prisoner undergoes a physical and psychological "softening-up" which includes: limited unpalatable food rations,withholding of tobacco,possible work details,severely inadequate use of toilet facilities, no use of facilities for personal cleanliness,limitation of sleep such as requiring a subject to sleep with a bright light in his eyes. Apparently the interrogation and autobiographical ,material, the reports of the prisoner's behaviour in confinement, and tentative "personality typing" by the interrogators, provide the basis upon which exploitation plans are made.

There is a major difference between preparation for elicitation and for brainwashing .Prisoners exploited through elicitation must retain sufficient clarity of thought to be able to give coherent,factual accounts. In brainwashing , on the other hand, the first thing attacked is clarity of thought. To develop a strategy of defense, the controlled individual must determine what plans have been made for his exploitation. Perhaps the best cues he can get are internal reactions to the pressures he undergoes.

The most important aspect of the brainwashing process is the interrogation. The other pressures are designed primarily to help the interrogator achieve his goals. The following states are created systematically within the individual . These may vary in order, but all are necessary to the brainwashing process:

1. A feeling of helplessness in attempting to deal with the impersonal machinery of control.

2. An initial reaction of "surprise."

3. A feeling of uncertainty about what is required of him.

4. A developing feeling of dependence upon the interrogator .

5. A sense of doubt and loss of objectivity.

6. Feelings of guilt.

7. A questioning attitude toward his own value-system.

8. A feeling of potential "breakdown," i.e.,that he might go crazy.

----

9. A need to defend his acquired principles.

10. A final sense of "belonging" (identification).

A feeling of helplessness in the face of the impersonal machinery of control is carefully engendered within the prisoner. The individual who receives the preliminary treatment described above not only begins to feel like an "animal" but also feels that nothing can be done about it. No one pays any personal attention to him. His complaints fall on deaf ears. His loss of communication, if he has been isolated, creates a feeling that he has been "forgotten." Everything that happens to him occurs according to an impersonal; time schedule that has nothing to do with his needs. The voices and footsteps of the guards are muted. He notes many contrasts,e.g.,his greasy,unpalatable food may be served on battered tin dishes by guards immaculately dressed in white. The first steps in "depersonalization" of the prisoner have begun. He has no idea what to expect. Ample opportunity is allotted for him to ruminate upon all the unpleasant or painful things that could happen to him. He approaches the main interrogator with mixed feelings of relief and fright.

Surprise is commonly used in the brainwashing process. The prisoner is rarely prepared for the fact that the interrogators are usually friendly and considerate at first. They make every effort to demonstrate that they are reasonable human beings. Often they apologize for bad treatment received by the prisoner and promise to improve his lot if he, too, is reasonable. This behaviour is not what he has steeled himself for. He lets down some of his defenses and tries to take a reasonable attitude. The first occasion he balks at satisfying a request of the interrogator , however, he is in for another surprise. The formerly reasonable interrogator unexpectedly turns into a furious maniac. The interrogator is likely to slap the prisoner or draw his pistol and threaten to shoot him. Usually this storm of emotion ceases as suddenly as it began and the interrogator stalks from the room. These surprising changes create doubt in the prisoner as to his very ability to perceive another person's motivations correctly. His next interrogation probably will be marked by impassivity in the interrogator 's mien.

A feeling of uncertainty about what is required of him is likewise carefully engendered within the individual . Pleas of the prisoner to learn specifically of what he is accused and by whom are side-stepped by

the interrogator. Instead, the prisoner is asked to tell why he thinks

----

he is held and what he feels he is guilty of. If the prisoner fails to come up with anything, he is accused in terms of broad generalities (e.g., espionage, sabotage,acts of treason against the "people"). This usually provokes the prisoner to make some statement about his activities. If this take the form of a denial, he is usually sent to isolation on further decreased food rations to "think over" his crimes. This process can be repeated again and again. As soon as the prisoner can think of something that might be considered self-incriminating, the interrogator appears momentarily satisfied. The prisoner is asked to write down his statement in his own words and sign it.

Meanwhile a strong sense of dependence upon the interrogator is developed. It does not take long for the prisoner to realize that the interrogator is the source of all punishment , all gratification,and all communication. The interrogator , meanwhile,demonstrates his unpredictbility. He is perceived by the prisoner as a creature of whim. At times, the interrogator can be pleased very easily and at other times no effort on the part of the prisoner will placate him. The prisoner may begin to channel so much energy into trying to predict the behaviour of the unpredictable interrogator that he loses track of what is happening inside himself.

After the prisoner has developed the above psychological and emotional reactions to a sufficient degree, the brainwashing begins in earnest. First, the prisoner's remaining critical faculties must be destroyed. He undergoes long, fatiguing interrogations while looking at a bright light. He is called back again and again for interrogations after minimal sleep. He may undergo torture that tends to create internal conflict. Drugs may be used to accentuate his "mood swings." He develops depression when the interrogator is being kind and becomes euphoric when the interrogator is threatening the direst penalties. Then the cycle is reversed. The prisoner finds himself in a constant state of anxiety which prevents him from relaxing even when he is permitted to sleep. Short periods of isolation now bring on visual and auditory hallucinations. The prisoner feels himself losing his objectivity. It is in this state that the prisoner must keep up an endless argument with the interrogator . He may be faced with the confessions of other individuals who "collaborated" with him in his crimes. The prisoner seriously begins to doubts his own memory. This feeling is heightened by his inability to recall little things like the names of the people he knows very well or the date of his birth. The interrogator patiently sharpens this feeling of doubt by more questioning. This tends to create a serious state of uncertainty when the individual has lost most of his critical faculties.

The prisoner must undergo additional internal conflict when strong feelings of guilt are aroused within him. As any clinical psychologist is aware, it is not at all difficult to create such feelings. Military servicemen are particularly vulnerable. No one can morally justify killing even in wartime. The usual justification is on the grounds of necessity or self-defense. The interrogator is careful to circumvent such justification. He keeps the interrogation directed toward the prisoner's moral code. Every moral vulnerability is exploited by incessant questioning along this line until the prisoner begins to question the very fundamentals of his own value-system. The prisoner must constantly fight a potential breakdown. He finds that his mind is "going blank" for longer and longer periods of time. He can not think constructively. If he is to maintain any semblance of psychological integrity, he must bring to an end this state of interminable internal conflict. He signifies a willingness to write a confession.

If this were truly the end, no brainwashing would have occurred. The individual would simply have given in to intolerable pressure. Actually, the final stage of the brainwashing process has just begun. No matter what the prisoner writes in his confession the interrogator is not satisfied. The interrogator questions every sentence of the confession. He begins to edit it with the prisoner. The prisoner is forced to argue against every change. This is the essence of brainwashing. Every time that he gives in on a point to the interrogator, he must rewrite his whole confession. Still the interrogator is not satisfied. In a desperate attempt to maintain some semblance of integrity and to avoid further brainwashing, the prisoner must begin to argue that what he has already confessed to is true. He begins to accept as his own the statements he has written. He uses many of the interrogator's earlier arguments to buttress his position. By this process,identification with the interrogator's value-system becomes complete. It is extremely important to recognize that a qualitative change has taken place within the prisoner. The brainwashed victim does not consciously change his value-system; rather the change occurs despite his efforts. He is no more responsible for this change than is an individual who "snaps" and becomes psychotic. And like the psychotic, the prisoner is not even aware of the transition.

DEFENSIVE MEASURES OTHER THAN ON THE POLICY AND PLANNING LEVEL

1. Training of Individuals potentially subject to communist control.

Training should provide for the trainee a realistic appraisal of what control pressures the communists are likely to exert and what the usual human reactions are to such pressures. The trainee must learn the most effective ways of combatting his own reactions to such pressures and he must learn reasonable expectations as to what his behaviour should be. Training has two decidedly positive effects; first, it provides the trainee with ways of combatting control; second, it provides the basis for developing an immeasurable boost in morale. Any positive action that the individual can take, even if it is only slightly effective, gives him a sense of control over a situation that is otherwise controlling him.

2. Training must provide the individual with the means of recognizing realistic goals for himself.

a. Delay in yielding may be the only achievement that can be hoped for. In any particular operation, the agent needs the support of knowing specifically how long he must hold out to save an operation, protect his cohorts, or gain some other goal.

b. The individual should be taught how to achieve the most favorable treatment and how to behave and make necessary concessions to obtain minimum penalties.

c. Individual behavioural responses to the various communist control pressures differ markedly. Therefore, each trainee should know his own particular assets and limitations in resisting specific pressures. He can learn these only under laboratory conditions simulating the actual pressures he may have to face.

d. Training must provide knowledge of the goals and the restrictions placed upon his communist interrogator. The trainee should know what controls are on his interrogator and to what extent he can manipulate the interrogator. For example, the interrogator is not permitted to fail to gain "something" from the controlled individual. The knowledge that, after the victim has proved that he is a "tough nut to crack" he can sometimes indicate that he might compromise on some little point to help the interrogator in return for more favorable treatment, may be useful indeed. Above all, the potential victim of communist control can gain a great deal of psychological support from the knowledge that the communist interrogator is not a completely free agent who can do whatever he wills with his victim.

e. The trainee must learn what practical cues might aid him in recognizing the specific goals of his interrogator. The strategy of defense against elicitation may differ markedly from the strategy to prevent brainwashing. To prevent elicitation, the individual may hasten his own state of mental confusion; whereas, to prevent brainwashing, maintaining clarity of thought processes is imperative.

f. The trainee should obtain knowledge about communist "carrots" as well as "sticks." The communists keep certain of their promises and always renege on others. For example, the demonstrable fact that "informers" receive no better treatment than other prisoners should do much to prevent this particular evil. On the other hand, certain meaningless concessions will often get a prisoner a good meal.

g. In particular, it should be emphasized to the trainee that, although little can be done to control the pressures exerted upon him, he can learn something about controlling his personal reactions to specific pressures. The trainee can gain much from learning something about internal conflict and conflict-producing mechanisms. He should learn to recognize when someone is trying to arouse guilt feelings and what behavioural reactions can occur as a response to guilt.

h. Finally, the training must teach some methods that can be utilized in thwarting particular communist control techniques:

Elicitation. In general, individuals who are the hardest to interrogate for information are those who have experienced previous interrogations. Practice in being the victim of interrogation is a sound training device.

Torture. The trainee should learn something about the principles of pain and shock. There is a maximum to the amount of pain that can actually be felt. Any amount of pain can be tolerated for a limited period of time. In addition, the trainee can be fortified by the knowledge that there are legal limitations upon the amount of torture that can be inflicted by communist jailors.

Isolation. The psychological effects of isolation can probably be thwarted best by mental gymnastics and systematic efforts on the part of the isolate to obtain stimulation for his neural end organs.

Controls on Food and Tobacco. Foods given by the communists will always be enough to maintain survival. Sometimes the victim gets unexpected opportunities to supplement his diet with special minerals,vitamins and other nutrients (e.g.,"iron" from the rust of prison bars). In some instances, experience has shown that individuals could exploit refusal to eat. Such refusal usually resulted in the transfer of the individual to a hospital where he received vitamin injections and nutritious food. Evidently attempts of this kind to commit suicide arouse the greatest concern in communist officials. If deprivation of tobacco is the control being exerted. the victim can gain moral satisfaction from "giving up" tobacco. He can't lose since he is not likely to get any anyway.

Fatigue. The trainee should learn reactions to fatigue and how to overcome them insofar as possible. For example, mild physical exercise "clears the head" in a fatigue state.

Writing Personal Accounts and Self-Criticism. Experience has indicated that one of the most effective ways of combatting these pressures is to enter into the spirit with an overabundance of enthusiasm. Endless written accounts of inconsequential material have virtually "smothered" some eager interrogators. In the same spirit, sober, detailed self-criticisms of the most minute "sins" has sometimes brought good results.

Guidance as to the priority of positions he should defend. Perfectly compatible responsibilities in the normal execution of an individual's duties may become mutually incompatible in this situation. Take the example of a senior grade military officer. He has the knowledge of sensitive strategic intelligence which it is his duty to protect. He has the responsibility of maintaining the physical fitness of his men and serving as a model example for their behaviour. The officer may go to the camp commandant to protest the treatment of the POWs and the commandant assures him that treatment could be improved if he will swap something for it. Thus to satisfy one responsibility he must compromise another. The officer, in short, is in a constant state of internal conflict. But if the officer is given the relative priority of his different responsibilities, he is supported by the knowledge that he won't be held accountable for any other behaviour if he does his utmost to carry out his highest priority responsibility. There is considerable evidence that many individuals tried to evaluate the priority of their responsibilities on their own, but were in conflict over whether others would subsequently accept their evaluations. More than one individual was probably brainwashed while he was trying to protect himself against elicitation.

CONCLUSIONS

The application of known psychological principles can lead to an understanding of brainwashing.

1. There is nothing mysterious about personality changes resulting from the brainwashing process.

2. Brainwashing is a complex process. Principles of motivation, perception, learning, and physiological deprivation are needed to account for the results achieved in brainwashing.

3. Brainwashing is an involuntary re-education of the fundamental beliefs of the individual. To attack the problem successfully, the brainwashing process must be differentiated clearly from general education methods for thought-control or mass indoctrination, and elicitation.

4. It appears possible for the individual,through training,to develop limited defensive techniques against brainwashing. Such defensive measures are likely to be most effective if directed toward thwarting individual emotional reactions to brainwashing techniques rather than toward thwarting the techniques themselves.

----

15 August 1955

===
(note Declassified)

SECRET

CENTRAL INTELLIGENCE AGENCY
WASHINGTON 25, D. C.

19 JUN 1964

(Commission No. 1131)

MEMORANDUM FOR: Mr. J. Lee Rankin

General Counsel
President's Commission on the
Assassination of President Kennedy

SUBJECT : Soviet Brainwashing Techniques

1. Reference is made to your memorandum of 19 May 1964, requesting that materials relative to Soviet techniques in mind conditioning and brainwashing be made available to the Commission.

2. At my request, experts on these subjects within the CIA have prepared a brief survey of Soviet research in the direction and control of human behavior, a copy of which is attached. The Commission may retain this document. Please note that the use of certain sensitive materials requires that a sensitivity indicator be affixed.

3. In the immediate future, this Agency will make available to you a collection of overt and classified materials on these subjects, which the Commission may retain.

4. I hope that these documents will be responsive to the Commission's needs.

(SIGNED)

(DECLASSIFIED) Richard Helms
(By C.I.A.) Deputy Director for Plans
(letter of ___________)
(---------------------)

Attachment

CD 1131 SECRET

MEMORANDUM

SUBJECT: Soviet Research and Development in the Field of
Direction and Control of Human Behavior.

1. There are two major methods of altering or controlling human behavior, and the Soviets are interested in both. The first is psychological; the second, pharmacological. The two may be

used as individual methods or for mutual reinforcement. For long-term control of large numbers of people, the former method is more promising than the latter. In dealing with individuals, the U.S. experience suggests the pharmacological approach (assisted by psychological techniques) would be the only effective method. Neither method would be very effective for single individuals on a long term basis.

2. Soviet research on the pharmacological agents producing behavioral effects has consistently lagged about five years behind Western research. They have been interested in such research, however, and are now pursuing research on such chemicals as LSD-25, amphetamines, tranquillizers, hypnotics, and similar materials. There is no present evidence that the Soviets have any singular, new, potent drugs to force a course of action on an individual. They are aware, however, of the tremendous drive produced by drug addiction, and PERHAPS could couple this with psychological direction to achieve control of an individual.

3. The psychological aspects of behavior control would include not only conditioning by repetition and training, but such things as hypnosis, deprivation, isolation, manipulation of guilt feelings, subtle or overt threats, social pressure, and so on. Some of the newer trends in the USSR are as follows:

a. The adoption of a multidisciplinary approach integrating biological,social and physical-mathematical research in attempts better to understand, and eventually, to control human behavior in a manner consonant with national plans.

b. The outstanding feature, in addition to the inter-disciplinary approach, is a new concern for mathematical approaches to an understanding of behavior. Particularly notable are attempts to use modern information theory, automata theory, and feedback concepts in interpreting the mechanisms by which the "second signal system," i.e., speech and associated phenomena, affect human behavior. Implied by this "second signal system," using INFORMATION inputs as causative agents rather than chemical agents, electrodes or other more exotic techniques applicable, perhaps, to individuals rather than groups.

c. This new trend, observed in the early Post-Stalin Period, continues. By 1960 the word "cybernetics" was used by the Soviets to designate this new trend. This new science is considered by some as the key to understanding the human brain and the product of its functioning--psychic activity and personality--to the development of means for controlling it and to ways for molding the character of the "New Communist Man". As one Soviet author puts it: Cybernetics can be used in "molding of a child's character, the inculcation of knowledge and techniques, the amassing of experience, the establishment of social behavior patterns...all functions which can be summarized as 'control' of the growth process of the individual." 1/Students of particular disciplines in the USSR, such as psychologist and social scientists, also support the general cybernetic trend. 2/ (Blanked by CIA)

4. In summary, therefore, there is no evidence that the Soviets have any techniques or agents capable of producing particular behavioral patterns which are not available in the West. Current research indicates that the Soviets are attempting to develop a technology for controlling the development of behavioral patterns among the citizenry of the USSR in accordance with politically determined requirements of the system. Furthermore, the same technology can be applied to more sophisticated approaches to the "coding" of information for transmittal to population targets in the "battle for the minds of men." Some of the more esoteric techniques such as ESP or, as the Soviets call it, "biological radio-communication", and psychogenic agents such as LSD,

are receiving some overt attention with, possibly, applications in mind for individual behavior control under clandestine conditions. However, we require more information than is currently available in order to establish or disprove planned or actual applications of various methodologies by Soviet scientists to the control of actions of articular individuals.

References

1. Itelson, Lev, "Pedagogy: An Exact Science?" USSR October 1963, p. 10.
2. Borzek, Joseph, "Recent Developments in Soviet Psychology," Annual Review of Psychology, Vol. 15, 1964, p. 493-594.

The first letter and attachment are from DECLASSIFIED DOCUMENTS 1984 microfilms under MKULTRA (84) 002258, published by Research Publication Woodbridge, CT 06525. Some original markings were not retyped, but the content is the same.

The second letter and attachment are from the Warren Commission documents. Notice should be paid to the different tone Helms gives to his letter, keeping in mind he was found guilty of lying to Congress. He places greater emphasis on "Soviet" practices and tries to diminish breakthroughs gained by Americans. Some thought should be given as to WHY the Warren Commission sought such documents (remembering that ALLEN DULLES was a member of that Commission). They were exploring the Manchurian candidate theory. It was revealed during the Church Committee hearings of 1975 that Helms had been in charge of Project AMLASH, a program to assassinate Castro (Cuba),Trujillo (Dominican Republic), Diem (RVN), Schneider (Chile) using MAFIA figures John Roselli and Santos Trafficante to do the job.

Care was used to insure lines appear in same length and order. Page length will have to be adjusted if you desire to print this. Look for other specials soon. David John Moses.

WHY SUSPECTS CONFESS

By

David D. Tousignant, M.A.
Inspector
Lowell, Massachusetts, Police Department

Many criminal cases, even when investigated by the most experienced and best qualified investigators, are ultimately solved by an admission or confession from the person responsible for committing the crime. Oftentimes, investigators are able to secure only a minimal amount of evidence, be it physical or circumstantial, that points directly to a suspect, and in many instances, this evidence is not considered strong enough by prosecutors to obtain a conviction. In such cases, the interrogation of the suspects and their subsequent confessions are of prime importance.

This article addresses the question of why suspects speak freely to investigators, and ultimately, sign full confessions. The physical and psychological aspects of confession and how they relate to successful interrogations of suspects are also discussed, as is the "breakthrough," the point in the interrogation when suspects make an admission, no matter how minuscule, that begins the process of obtaining a full confession.

DEFINING INTERROGATION

Interrogation is the questioning of a person suspected of having committed a crime. (1) It is designed to match acquired information to a particular suspect in order to secure a confession. (2) The goals of interrogation include:

* To learn the truth of the crime and how it happened

* To obtain an admission of guilt from the suspect

* To obtain all the facts to determine the method of operation and the circumstances of the crime in question

* To gather information that enables investigators to arrive at logical conclusions

* To provide information for use by the prosecutor in possible court action. (3)

Knowing the definition and objectives of the interrogation, the question then asked is, "Why do suspects confess?" Self-condemnation and self-destruction are not normal human behavioral characteristics. Human beings ordinarily do not utter unsolicited, spontaneous confessions. (4) It is logical to conclude, therefore, that when suspects are taken to police stations to be questioned concerning their involvement in a particular crime, their immediate reaction will be a refusal to answer any questions. With the deluge of television programs that present a clear picture of the Miranda warning and its application to suspects, one would conclude that no one questioned about a crime would surrender incriminating information, much less supply investigators with a signed, full confession. It would also seem that once suspects sense the direction in which the investigators are heading, the conversation would immediately end. However, for various psychological reasons, suspects continue to speak with investigators.

SUSPECT PARANOIA

Suspects are never quite sure of exactly what information investigators possess. They know that the police are investigating the crime, and in all likelihood, suspects have followed media accounts of their crimes to determine what leads the police have. Uppermost in their minds, however, is how to escape detection and obtain firsthand information about the investigation and where it is heading.

Such "paranoia" motivates suspects to accompany the police voluntarily for questioning. Coupled with curiosity, this paranoia motivates suspects to appear at police headquarters as "concerned citizens" who have information pertinent to the case. By doing this, suspects may attempt to supply false or noncorroborative information in order to lead investigators astray, gain inside information concerning the case from investigators, and remove suspicion from themselves by offering information on the case so investigators will not suspect their involvement.

For example, in one case, a 22-year-old woman was discovered in a stairwell outside of a public building. The woman had been raped and was found naked and bludgeoned. Investigators interviewed numerous people during the next several days but were unable to identify any suspects. Media coverage on the case was extremely high.

Several days into the investigation, a 23-year-old man appeared at police headquarters with two infants in tow and informed investigators that he believed he may have some information regarding the woman's death. The man revealed that when he was walking home late one evening, he passed the area where the woman was found and observed a "strange individual" lurking near an adjacent phone booth. The man said that because he was frightened of the stranger, he ran back to his home. After reading the media accounts of the girl's death, he believed that he should tell the police what he had observed.

The man gave police a physical description of the "stranger" and then helped an artist to compose a sketch of the individual. After he left, investigators discovered that the sketch bore a strong resemblance to the "witness" who provided the information.

After further investigation, the witness was asked to return to the police station to answer more questions, which he did gladly. Some 15 hours into the interrogation, he confessed to one of his "multiple personalities" having killed the woman, who was unknown to him, simply because the victim was a woman, which is what the suspect had always wanted to be.

This case clearly illustrates the need for some suspects to know exactly what is happening in an investigation. In their minds, they honestly believe that by hiding behind the guise of "trying to help," they will, without incriminating themselves, learn more about the case from the investigators.

INTERROGATION SETTING

In any discussion concerning interrogation, it is necessary to include a review of the surroundings where a suspect is to be interrogated. Because there is a general desire to maintain personal integrity before family members and peer groups, suspects should be removed from familiar surroundings and taken to a location that has an atmosphere more conducive to cooperativeness and truthfulness. (5) The primary psychological factor contributing to successful interrogations is privacy--being totally alone with suspects. (6) This privacy prompts suspects to feel willing to unload the burden of guilt. (7) The interrogation site should isolate the suspect so that only the interrogator is present. The suspect's thoughts and responses should be free from all outside distractions or stimuli.

The interrogation setting also plays an important part in obtaining confessions. The surroundings should reduce suspect fears and contribute to the inclination to discuss the crime. Because fear is a direct reinforcement for defensive mechanisms (resistance), it is important to erase as many fears as possible. (8) Therefore, the interrogation room should establish a business atmosphere as opposed to a police-like atmosphere. While drab, barren interrogation rooms increase fear in suspects, a location that displays an open, you-have-nothing-to fear quality about it can do much to break down interrogation defensiveness, thereby eliminating a major barrier. (9) The interrogators tend to disarm the suspects psychologically by placing them in surroundings that are free from any fear-inducing distractions.

PSYCHOLOGICAL FACTORS

More than likely, suspects voluntarily accompany investigators, either in response to a police request to answer questions or in an attempt to learn information about the investigation. Once settled in the interrogation room, the interrogators should treat suspects in a civilized manner, no matter how vicious or serious the crime might have been. While they may have feelings of disgust for the suspects, the goal is to obtain a confession, and it is important that personal emotions not be revealed. (10)

Investigators should also adopt a compassionate attitude and attempt to establish a rapport with suspects. In most cases, suspects commit crimes because they believe that it offers the best solution to their needs at the moment. (11) Two rules of thumb to remember are: 1) "There but for the grace of God go I"; and 2) it is important to establish a common level of understanding with the suspects. (12) These rules are critical to persuading suspects to be open, forthright, and honest. Suspects should be persuaded to look beyond the investigators' badges and see, instead, officers who listen without judging. If investigators are able to convince suspects that the key issue is not the crime itself, but what motivated them to commit the crime, they will begin to rationalize or explain their motivating factors.

At this stage of the interrogation, investigators are on the brink of having suspects break through remaining defensive barriers to admit involvement in the crime. This is the critical stage of the interrogation process known as the breakthrough.

THE BREAKTHROUGH

The breakthrough is the point in the interrogation when suspects make an admission, no matter how small. (13) In spite of having been advised of certain protections guaranteed by the Constitution, most suspects feel a need to confess. Both hardcore criminals and first-time offenders suffer from the same pangs of conscience. (14) This is an indication that their defense mechanisms are diminished, and at this point, the investigators may push through to elicit the remaining elements of confession.

In order for interrogators to pursue a successful breakthrough, they must recognize and understand certain background factors that are unique to a particular suspect. Many times, criminals exhibit psychological problems that are the result of having come from homes torn by conflict and dissension. Also frequently found in the backgrounds of criminals are parental rejection and inconsistent and severe punishment. (15) It is important that investigators see beyond the person sitting before them and realize that past experiences can impact on current behavior. Once interrogators realize that the fear of possible punishment, coupled with the loss of pride in having to admit to committing mistakes, is the basic inhibitor they must overcome in suspects, they will quickly be able to formulate questions and analyze responses that will break through the inhibitors.

SUCCESSFUL INTERROGATIONS

Investigators must conduct every interrogation with the belief that suspects, when presented with the proper avenue, will use it to confess their crimes. Research indicates that most guilty persons who confess are, from the outset, looking for the proper opening during the interrogation to communicate their guilt to the interrogators. (16)

Suspects confess when the internal anxiety caused by their deception outweighs their perceptions of the crime's consequences. (17) In most instances, suspects have magnified, in their minds, both the severity of the crime and the possible repercussions. Interrogators should allay suspect anxiety by putting these fears into perspective.

Suspects also make admissions or confessions when they believe that cooperation is the best course of action. (18) If they are convinced that officers are prepared to listen to all of the circumstances surrounding the crimes, they will begin to talk. The psychological and physiological pressures that build in a person who has committed a crime are best alleviated by communicating. (19) In order to relieve these suppressed pressures, suspects explain the circumstances of their crimes they confess.

And, finally, suspects confess when interrogators are able to speculate correctly on why the crimes were committed. Suspects want to know ahead of time that interrogators will believe what they have to say and will understand what motivated them to commit the crime.

CONCLUSION

It is natural for suspects to want to preserve their privacy, civil rights, and liberties. It is also natural for suspects to resist discussing their criminal acts. For these very reasons, however, investigators must develop the skills that enable them to disarm defensive resistors established by suspects during interrogation. Before suspects will confess, they must feel comfortable in their surroundings, and they must have confidence in the interrogators, who should attempt to gain this confidence by listening intently to them and by allowing them to verbalize their accounts of the crimes.

Interrogators who understand what motivates suspects to confess will be better able to formulate effective questions and analyze suspect responses. Obviously, more goes into gaining a confession than is contained in this article. However, if the interrogator fails to understand the motivations of the suspect, other factors impacting on obtaining the confession will be less effective.

FOOTNOTES

(1) Charles E. O'Hara and Gregory L. O'Hara, Fundamentals of Criminal Investigation, 5th ed. rev. (Springfield, IL: Charles C. Thomas, 1988), p. 117.

(2) W. E. Renoud, Criminal Investigation Digest (Springfield, IL: Charles C. Thomas, 1981), p. 10.

(3) John J. Horgan, Criminal Investigations, 2d ed. (New York, NY: McGraw-Hill Book Company, 1979), p. 78.

(4) Fred E. Inbau, John E. Reid, and Joseph P. Buckley, Criminal Interrogation and Confessions, 3d ed. (Baltimore, MD: Williams & Wilkins, 1986), p. 16.

(5) Robert F. Royal and Steven R. Schutt, The Gentle Art of Interviewing and Interrogation: A Professional Manual and Guide (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1976), p. 56.

(6) Supra note 4, p. 24.

(7) Charles R. Swanson, Jr., Neil Chamelin, and Leonard Territo, Criminal Investigation, 4th ed. (New York, NY: Random House, 1988), p. 210.

(8) Supra note 5, p. 57.

(9) Ibid.

(10) Supra note 2, p. 12.

(11) Ibid., p. 13.

(12) Ibid., p. 13.

(13) Supra note 5.

(14) Supra note 7.

(15) James C. Coleman, James N. Butcher, and Robert C. Carson, Abnormal Psychology and Modern Life, 7th ed. (Glenview, IL: Scott Foresman and Company, 1984), p. 261.

(16) Supra note 7, p. 209.

(17) John Reid and Associates, The Reid Technique of Interviewing and Interrogation (Chicago, IL: Reid & Associates, 1986), p. 44.

(18) Supra note 5, p. 115.

(19) Supra note 7, p. 209.

CELLULAR TELEPHONE PHREAKING

How would ya like to have a phone that no body could locate? How bout free phone service on it too? Well Cellular telephones have the potential to do all this and more. First lets discuss some basics of the service.
Q:What is cellular a cellular phone?
A: A 800 mhz radiotelephone, running 3 watts, with the ability to change channel on computer command from the central switch. This happens when you travel thru the service area and your signal becomes stronger at a neighboring cell base station.
Q: They are marketed as a high security device with no possibility of anyone making a phoney call and charging it to someone else, how can it be phreaked?
A: An understanding of the phone reveals that every time a call is made, the phone number,an electronic serial number, and other data is sent to the switch. If you were to listen to the oposite side of the control channel as the call is being "set-up" you would hear this data being transmitted to the switch in NRZ code (non-return to zero). All one has to do, is record this info and program the bogus phone to these params and a free call is possible thru the switch.
Q: Has anyone done this yet?
A: YES, about 6 months after the first cellular phone system was "turned-up" a technician programmed a panasonic telephone with a NEC E.S.N. (Electronic

serial number) this was reportedly done for a gram of coke. With the popular ROM programmers available today, almost any NAM (Numeric Assignment Module) can be duplicated or copied with changes. (The NAM is the heart of the billing information and contains the phone number but not the ESN) The most popular integrated circut for NAMs is the 74LS123.

Q: This sounds like a lot of trouble, is there easier ways to get service?

A: SURE, the cellphone companies have been their own downfall. In an effort market their wares as universal service (Your phone will work in any system) they have let the cart get before the horse. Nobody can tell if a phone from another city (that has a roaming agreement) is valid till its too late. The only thing they could do after finding out is block any call with the bad ESN because as we know, the phone number is easy to change, but the ESN is not. So heres a likely plot...a roamer identifying itself as a number from Chicago non-wireline accesses a Cellular system in Dallas. Sometimes an operator intervienes but you can bullshit them as long as you know the information you have programmed into your phone. Then you make calls just like you are a local user. If you're found out, you remove the number, change it to another, and see if that works. Usualy it will require the radio's ESN chip to be changed, but thats a lot easier if you have a ZIF (zero insertion force) socket installed, thats what I use.

SCANNER CONVERTERS FOR CELLULAR TELEPHONE

This article is presented for information only. The new Electronic Communications Privacy Act makes it illegal to monitor cellular telephone calls.

A UHF TV tuner can be used as a converter to listen to cellular telephone calls. Salvage a UHF tuner from and old TV set. Connect it to a power supply. Typical voltage requirements are 12 - 25 volts. If the set is still working, measure the voltage before removing the tuner. Connect the output cable from the tuner to the external antenna input of a scanner or tunable monitor. Tune the scanner or monitor to a frequency between 41 and 46 MHz which is the IF output of the tuner. If you are within a few miles of a base station, a pair of test leads clipped to the antenna terminals of the tuner will serve as an antenna. Turn off the squelch on the scanner or monitor and carefully tune through UHF channels 70 - 83.

It is easier to use a tunable monitor than a scanner for this application because the monitor allows you to compensate for drift in the tuner. Either will provide an adequate means of checking out the cellular activity in your area.

There are several crystal controlled converters available which will convert cellular frequencies to the UHF range of many scanners. There is a slight problem involved with these. The spacing between cellular frequencies is 30 KHz. Most scanners have a stepping interval of 12.5 Khz at UHF. This means that on most channels the frequency tuned to by the scanner will not be a perfect match. I have been assured by one of the converter manufacturers that this is not a serious problem. When using this type of converter, the scanner can be used in scan or search modes as usual.

I wanted to find out how much discrepancy exists between the output of the converters and the tuning intervals of most scanners. I took the specs of a typical converter and put my computer to work doing the calculations. What follows is the result of this examination. Listed are the cellular base frequencies followed by the frequencies after conversion followed by the closest tuning point of a scanner with a tuning interval of 12.5 KHz. Each of the base frequencies listed is paired with a mobile frequency located 45 MHz lower. The mobile frequencies are not listed.

All 666 base frequencies were checked. Only the first 33 of these are listed. The pattern repeats throughout the list.

CELLULAR FREQ. CONVERTER OUT CLOSEST SCANNER FREQ.

870.030	486.030	486.0250
870.060	486.060	486.0625
870.090	486.090	486.0875
870.120	486.120	486.1250
870.150	486.150	486.1500
870.180	486.180	486.1750
870.210	486.210	486.2125
870.240	486.240	486.2375
870.270	486.270	486.2750
870.300	486.300	486.3000
870.330	486.330	486.3250
870.360	486.360	486.3625
870.390	486.390	486.3875
870.420	486.420	486.4250
870.450	486.450	486.4500
870.480	486.480	486.4750
870.510	486.510	486.5125
870.540	486.540	486.5375
870.570	486.570	486.5750
870.600	486.600	486.6000
870.630	486.630	486.6250
870.660	486.660	486.6625
870.690	486.690	486.6875
870.720	486.720	486.7250
870.750	486.750	486.7500
870.780	486.780	486.7750
870.810	486.810	486.8125
870.840	486.840	486.8375
870.870	486.870	486.8750
870.900	486.900	486.9000
870.930	486.930	486.9250
870.960	486.960	486.9625
870.990	486.990	486.9875

CELLULAR FRAUD VERY PREVENTABLE,
ACCORDING TO AUDIOVOX PRESIDENT

(BPS) -- Eighteen people arrested last week in New York on charges of illegally using their cellular telephones would have been unable to commit such a crime had they been using cellular phones from Audiovox Corp., according to John Shalam, president of Audiovox.

The 18 were arrested on charges of illegally altering memory chips in their mobile phones so they could make calls without being charged.

"The sad thing is that this crime is very preventable," Shalam said. "If this type of alteration is attempted on an Audiovox cellular phone, the phone is rendered useless."

According to Louis Antoniou, vice president of Audiovox's mobile electronics division, such tampering is prevented on Audiovox phones by an algorithm built into the software which prevents alteration of the phone's electronic serial number (E.S.N).

"If someone attempts to change the E.S.N. without using the algorithm, the phone will not activate," Antoniou said. "As far as we know, such prevention against tampering is unique to Audiovox."

Cellular phones have memory chips which contain both a mobile identification number (M.I.N.) and the E.S.N. When a call is made, both the numbers are transmitted to the mobile carrier where a computer checks the validity of the E.S.N. If the number is valid, the call goes through and the cost is charged to a billing number provided by the M.I.N. chip.

By reprogramming the E.S.N., those arrested apparently caused other people to be billed for their calls.

Officials estimate that the fraud cost local mobile telephone companies approximately $40,000 per month. Nationwide, carriers were losing an estimated $3 million.

Audiovox Corp., a major supplier of cellular telephones, autosound and auto security products, is located at 150 Marcus Blvd., Hauppauge, NY 11788, (516) 249-3366.

The Charging Box

What it does:

The Charging Box is used to indicate when a call is being charged for and when it is not. Once installed, the box has two lights, a green and a red. Green means free and red shows that you are being stung by BT!

Components:

1 x green LED
1 x red LED
2 x short lengths of wire

1 x circuit board
2 x 10K ohm (1/4 watt) resistors
2 x small bulldog clips

Circuit Diagram:

```
             |  Line  |
             |  (50v) |
        |------        ------|
|                 |
|-----[]------O------|
|                 |
|-----[]------O------|
```

Where [] is a resistor and O is an LED.
NB. IMPORTANT! One LED should have it's anode towards the resistor
and the other should have it's cathode towards the
resistor.

Connection:

Build that onto the board and connect the two points marked line to the wire, with the bulldog clips at the end. The box should now be connected to the line in parallel with the phone.

Operation:

When the line is opened (Ie. the phone lifted) the green LED will light (if the read one does then just reverse the polarity of the box). Dialling numbers (by pulse) will cause the green LED to flicker but while you are making free calls it should never go out and the red LED will not light. As soon as the exchange starts charging for your call, the green LED will go out and the red LED glow.

How it works:

As the LEDs are in opposite directions, only one can light depending on the polarity of the current supply. This is exploited when the exchange begins charging as the polarity of the line is reversed.

- What To Look For In A Code Hacking Program -

Phreaking's getting tricky these days, ain't it?

Ok, there are two groups of things a code hacker should have, the necessities and the things that are good to have... Here are the necessities:

Mutliple ports. If you constantly try to hack from the same port (the 800/950 or whatever number that the company you're hacking from is on) you are begging to be caught. The program should have an option to handle at least 5 different ports. It should also be able to handle a different format for each one if necessary. (One could require nine digits, another only 4, another requiring a 9 before the place you're trying to call to, etc)

Multiple targets. The program should be able to handle as many target numbers as it can ports. If everytime you try a code you go to the same number you are, again, begging to be caught.

The ability to hack codes RANDOMLY. And when I say random, I mean going as far as to have a different seed each time it generates a random code... If you hack sequentially I hope you get caught.

Not only should the codes it tries be random, but almost everything about the program should be random. It should pick a random port, with a random target, and with a random code. Believe it or not, some companies are starting to show some intelligence, and they're beginning to notice patterns. . .
You can't predict chaos, remember that.

The ability to stop after a certain number of tries, or a certain number of successful codes, or at a certain time. If you let the hacker run for a long time, you better have a LOT of ports and targets set up... Hack for short periods of time, or for a relatively small number of tries. If you get impatient and desperate for codes, you will make mistakes.

And now, the nice things to have.

The ability to have a random delay between the tones it dials. Humans can't dial 11 digit numbers in .7 of a second, and the companies know that. Humans also cannot dial with a consistent gap between each tone. If the program puts a random time between each tone, the system will have a better chance of thinking you're a human.

The program SHOULD be able to encrypt all of the codes it hacks when it saves them/prints them/etc. That way, IF you get busted, you won't have so much evidence against you. When you get nailed, they go through everything, even if they are idiot schmucks. If your list of codes contains all 'wrong' codes, they'll have less of a case against you.

It is also nice if the code hacker waits a random length of time between attempts, no matter how many ports it is trying. If you're hacking random ports, with random targets, with a random delay between digits dialed, with a random amount of time between all of your attempts, and with a randomly generated code, you're going to be hard as hell to catch.

And now some warnings. . .

I don't know if it is a COMMON practice, but some companies have set up bad accounts (codes, whatever) for the specific purpose of catching whoever tries to use it. If it doesn't belong to a real person, only a hacker would get it.

Don't hack fast... If at all possible, dial fairly slowly. I've heard of places that watch for extremely fast dialers.

Don't phreak to the same place with the same code constantly. I feel that one is self explanatory.

If you're very cautious, you can always use someone else's line when you are searching for codes. But be SURE you don't leave anything that can point to you.

If you think there is a chance that you've been snagged, or at least caught the attention of the Gestapo, stop phreaking. The less stuff they have against you, the less of a case they'll have against you. Also, if you keep phreaking, they'll sooner or later shove a printout in your face that contains every number dialed from your phone. Don't bring everybody else down just because you got careless.

Speaking of bringing everyone else down... I don't know if the truth has been out yet, so I'll bring it out. There was a loser by the name of Jeremy Hall. His common handles were "Quicksilver" and "Shells". He thought he was hot shit. He set up many Alliance conferences, called up Voice Mailboxes almost everyday, etc. He was about 13 years old, a little whiny brat.
Well, there was also a damn good phracker by the handle of Amadeus. Ever

wonder what happened to him? Quicksilver turned him in to save his own ass. He also caused alot of Mailboxes to come down, and I think a few boards came down because of his ignorance.

[=] Everything you really never wanted to know about Coin Services & more! [=]
=-

Three basic types of coin services are available: semi-postpay, prepay, and local repay toll postpay.

A] Semipostpay Coin Service.
=-=-=-=-=-=-=-=-=-=-=-=-=-=-

1) When the telephone receiver is removed from the payphone, dail tone is returned to the caller. After the telephone user completed dialing and the connection to the called line is established, the telephone user listens to determine when the call is answered. Upon answer, the transmitter in the pay phone is disabled and coversation is inhibited. The phone user must then depoit a coin to enable the transmitter, thereby permitting conversation. Once a coin has been deposited, it cannot be returned.

2) On calles from semipostpay coin lines to the operator, a special paystation identification tone is given to the operator on answer. (This tone is controled by class-of-service assignment.) If supervision is not given, conversation is allowed on calles to the operator as well as other lines with a free terminating class of service.

3) Semipostpay coin service requires no special DCO system equipment, and operator rering capability is permitted.

B] Prepay Coin Service.
=-=-=-=-=-=-=-=-=-=-=-=

1) Prepay coin sevice provides coin collect, coin return, and rering capability (GREEN BOX). The DCO system does not require special prepay trunks or trunk groups.

2) On local calls, coins are automatically collected on completeted calls and returned on incompleted calls.   On toll calls, the operator has *FULL* control of coin collect, coin return, and rering functions. Any coin not returned by the operator will be collected on disconect.

3) Two basic methods are used for operator control of paystations in the DCO system: inband signaling and multiwink signaling. For inband signaling, coin collect, refund, and rering functions are controlled by MF signals applied to the voice path. For multiwink signaling, coin collect and refund signals are controlled by a series of up to five supervisory winks (momentary on-hook signals). (See following chart for inband and multiwink signaling arrangments.)

4) A + or - 130volt power supply is required for prepay station operation to provide coin collect and coin refund voltages. In addition, certain types of paystation instruments also require a +48volt supply.

TYPE	INBAND SIGNALING	MULTIWINK SIGNALING
Coin first	-Rotary dial, except W.E.1C	W.E.1C
	-Rotary dial W.E.1C	Other than W.E.1C
	-DTMF	
Dial Tone first	-Rotary dial, except W.E.1C	W.E.1C
	-Rotary dial W.E.1C	Other than W.E.1C
	-DTMF	

C] Local Prepay/Toll Postpay Service
=-=-=-=-=-=-=-=-=-=-=-=-=-=-==-=-=-=

1) Prepay line circuits and circuit unit assemblies are required for coin collect and refund on local calls. Local prepay service requires a coin deposit before dialing can proceed. On local calls, coins are automatically collected when the called party answeres. On toll calls, the initial deposit is returned before the operator answers.

2) Answer provides reverse battery supervision, which locks the coin mechanism of the payphone in the collect position. Deposits made on operator instruction are not refundable.

Coin Service, Prepay Coin on DSU-Remote (DSUR).
=-=

Prepay coin service for the DSUR is accomplished in the same fashion as in the DCO system. A maximum of prepay paystations are allowed per DSUR. (See the apove chart for inband and multiwink signaling arrangements.)

Miscellaneous Techniques for the Telecommunications Hobbyist

The purpose of this text-file is to explain the ethics and purpose of phone phreaking and hacking to the ones that don't know or that think they do but really don't. Also I will report on a few odd developments in the hack and phreak worlds, so this file is by no means just reserved to the newcomers. But most of it, however, is on the basic level. In later volumes I will get into more in-depth subjects. For the beginner, I will not get into basic telephony, switching systems and explaining basics such as loops, divertors, etc., but for those that need that information I highly recommend reading BIOC Agent's gem of a series, "The Basics of Communications". Though the earliest ones date back to 1983, they are very informative and well written. At the end of this file I'll put a little bibliography with a list of text-files and books that are recommended reading. Now on to the rest of the file, which will be roughly divided into sections.

I. Elitism. (This is the only section devoted entirely to newcomers.
Others can go ahead to section II).

It's funny listening to some of the new "phreaks" nowadays.

ALL NEW HACKERS/PHREAKS. . .LISTEN!

What hackers/phreaks do is illegal! Sort of like the mafia - if you turn someone in you can expect to get hurt! So, for all you people out there who cannot handle it, I suggest that you had better stop right away before you get yourself in trouble. There's too many kids out there today who think that they're big shit because they can make long distance calls for free... WHOOPIE! A phreak is not a person that makes long distance calls for nothing. Get that through your heads! A phreak is a person that experiments with the phone company, and tries to manipulate it and see what it can do! It only curtails 20% of long distance calls. That 20% is the final chapter of the phreak, once they crack the Bell system they can make calls for nothing.
HOW CAN ANYONE READ THE LAST CHAPTER AND KNOW WHAT THE BOOK CONTAINS?

Phreaking is illegal and you can get busted for it. No, the FBI won't bust you for sending someone a $2,000.00 phone bill, the FBI has nothing to do with that at all! And enough about MCI and tracing... 800 numbers always ANI! 950's are routed in a different way, otherwise they're the SAME as other prefixes! ANY number can trace, so there isn't one safe method or long distance company to make free calls. So if you are scared of getting caught, SIMPLY DO NOT DO IT! People who break into computer systems to crash and destroy them or use long distance codes for the mere sake of running up someone's bill should be caught. It's vandalism.

Also, a note about boxing. The blue box is the first and one of the few "boxes" [which is contradictory to the pirates and others that have a rainbow assortment of them], although I would also classify the black box as a "box". Others are just tools of the phone phreak. A beige box is nothing more than a lineman's handset, and a clear box is just a tone dialer. Also, boxing is not completely extinct, like some say. And YES, there ARE ways around ESS! One just has to look for them. Not everything one learns can be attained from a text-file. Phreaking is not a passive activity, one must go places, do things, and experiment. Although I am not saying that boxing is in it's prime, either. [I wasn't a phreak when boxing was in its prime, which was way back in the early 70's]. Phreaks still have blue boxes, some for sentimental reasons, and others still use them. A lot of the "boxes", such as the yellow, urine, lunch, super, cereal, plaid, brown, et. al., don't exist. They were "invented" by intelligent people for the plain idiots and "new breed" of what I call "c0mpyooter kidz" to toy with (and try to build and use!) Oh, and then there's boxes like the red box. The red box exists, but it's just a few of the tones in a blue box. So if you have a blue box, you also have a red box.

What else... Oh, yeah, something about codes. For your own saftey, never use codes posted on a BBS. Who knows how many people are using it. And, contradictory to the pirate's favorite little saying, "There's safety in numbers," it's actually more dangerous to use a code posted around the nation. All you have to do it put your code hacker on one night, and if you get about 4 codes, that should last you two months if you use one code every two weeks, and don't give any to anyone.

II. Trashing

Trashing, if done correctly, can be a very profitable and enjoyable part of a phreak's activities. After trashing local Bell and AT&T sites for over two years, I've gained a bit of experience on the subject, and have a few fairly good guidelines for trashing:

1)First of all, you need a place to trash. The best places are your local central office, business office, AT&T service branch, or communications center. To find out where these are located, just open up the good ol' white pages to "American Telephone and Telegraph" or "Bell Systems" and you will find several local addresses. When you pick one out that you think will be profitable, jot down the address and take a few drives out there;one during a weekday business hour, one on a Sunday, and another at night. This will give you an idea of how heavily populated it is at certain times. Don't get out of the car during these surveillance trips, but just make a note of security, etc. Some telco installations keep their trash locked up, others have it guarded, but most of them just have a plain old dumpster. During these trips you also have to watch when the trash is collected, so that you can arrange a day when the trash will be at its peak.

2)Once you have a site picked out, and a good time and date to go, drive out with a friend or two. Sometimes it's better to park your car and walk when it is guarded, so you will have a smaller chance of being detected, but most of the time you can just drive right up. Always do it at night, Fridays, Saturdays and Sundays being the best. Once you are at the dumpster, grab all the bags and put them in the trunk. If you walked, then take them out and leave as soon as possible. Not only is this safer (no worry about getting caught by the cops) than going in the dumpster and sorting the trash there, but it assures you that you don't miss anything. And what's nice about telco trash is that the worst it gets is coffee grounds or an apple core, so you won't have to worry about smelly garbage.

3)Drive off to your house and sort it in your garage, backyard, or whatever. Have some trash bags nearby to put the real trash in. The good trash you can then keep, and dispose of the rest.

There are many good things you can find in telco trash. There are always abundances of printouts, from loop tests to miscellaneous reports. Depending on exactly what kind of building you trashed, you could find broken phones (the parts are very useful) to blank letterheads. I have never found a pad of unused Bell letterheads, but if you find one that is in good condition but written on, take it to your local printer and have them print you out two dozen copies in the same color, but to omit the part that was written on. If the printer questions you, just leave and go somewhere else. At my local printer, this cost me $2.60. Letterheads and envelopes are very useful for scaring enemies (on occasion, friends too!), or for impressing phellow phreaks when writing to them. In Bell trash you can also find notebooks and binders with the Bell logo. Once I trashed a computer store and found a binder with the Intel logo on it. It now sits next to my PC and I use it to keep my technical information.

III. Your Phriends at Bell!

There's a lot of phree presents AT&T has for you that's just as easy as a phone call away:

Ever want more than one phone book? Is yours old and tattered? You can get a White Pages, Yellow Pages, Business-to-Business Yellow Pages, or whatever suburb yellow/white pages you want just by asking! It's very simple, and perfectly legal - just open the cover of your current White Pages and get the number to your local Administrative Office. Give 'em a call and ask for whatever phone book you want, and they'll send it free of charge. Don't order more than 3 at a time, however.

A way to get Bell stationary without going trashing is to call Bell and ask for information on, for instance, WATS lines. You'll get a little pamphlet in the mail about WATS lines, plus a Bell memorandum slip saying something like, "George --- here's the information you requested on WATS lines". As before, take it to your printers', and have it copied without the writing.

Those manhole covers that you see on your street with the words "Bell System" on it have more in there than you think. If you can lift one up using a crowbar, go inside. Sometimes you might find a telephone handset, and if you're lucky, a Bell manual or two describing the wires lining the inside. But most of the time, that's just a phreak phairy tale. It's not that easy, but I worked out an easy method to get various manuals that WORKS:
Ever see those little black lids on the corner of the block that says "Telephone" on it, and you open it up and there's a long wire in it? It's called a bridging head. Well go to one close to you, either if you have one or try one a few houses away. Take the lid off, and pitch it. Then call up repair service and say, "Hello, this is [insert the name of someone that lives near it, or bullshit a name], and I have a box at the corner of my house that contains phone wires. Well, I just looked outside and the lid is missing. I have a 6 year old daughter, and she plays outside a lot. I don't want her to get electrocuted or hurt, so could you please send someone out to replace the lid? My address is [fill in address here]." And in a while (they'll tell you the time), a bell lineman will drive up, open his truck and get out a replacement lid. When he's doing that, just reach in the truck and swipe something. But you have to be quick and accurate, and you can't be too choosy. While you're at it, you might as well get into a conversation with the guy. BSing with these people can sometimes yield good results.

Many of the Directory Assistance ops can easily be talked to. Although they get a lot of calls (1000-1300 a day), they still will talk for a few minutes. The problem is that they don't have access to much. They can tell you if a number is unlisted or not, and that's about it. The CN/A operator can give you the name and address of a number. And, if done correctly, you can get some information from her. I hear that most CN/As are going to become a regular customer pay service in the near future, due to all the teens already abusing them. My CN/A (614) doesn't even give you the full address or name on most of the numbers, they just tell you the major city it's in (like for a 614 number they'll say "that's in Columbus", and for a 216 number they'll say "that's in Cleveland"), which doesn't help at all. For unlisted numbers they'll tell you that they have no record. Some CN/As are on Microfische(like mine), and that's what happens when you call them. The others are computerized but they ask for a pass code (two letters and two numerals). It won't be long before this once-valuable operator becomes useless.

IV. Exchange Scanning

The best way to find pbxes, loops, and other goodies is to manually scan for them. In the NPA-NXX-99XX numbers, there's a lot of Bell goodies, just waiting for you to explore them. Get a notebook for phreaking and make a chart for each prefix like this (thanks to BIOC Agent 003 for this method):

```
                 NPA-NXX-99XX Scan
 ____________________________________________________________________________
|99x    x>| 0    |1     |2     |3     |4     |5     |6    |7    |8    |9    |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|990     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|991     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|992     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|993     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|994     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|995     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|996     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|997     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|998     |     |     |     |     |     |     |     |     |     |     |
|---------+------+------+------+------+------+------+-----+-----+-----+-----|
|999     |     |     |     |     |     |     |     |     |     |     |
|_________|______|______|______|______|______|______|_____|_____|_____|_____|
```

Then make a key something like:

R = ring [try again later]

B = busy ["   "   "]

R1= recording 1 [make a list of all that you come across, R1, R2, R3, etc.]

D = dial tone

O = intercept operator

S = sweep tone

T = tone [tone at lower number + ignore it's a loop]

I = ignore [dead silence. at higher number, it's a loop]

V = voice number to telco

C = carrier [modem]

Q = strange tone/clicks/buzzing

M = voice mail system

N = SCC / Network port (MCI, Sprint, etc)

Dial all the numbers on your sheet, and record your findings on the chart in your notebook. Another area that has a lot of things are the <800>/9XX-9999 series of numbers. At the time of this writing, most are disconnected, but a few useful numbers are still there. Also, <800>/NXX-10XX tend to yield with a lot of good findings. Try to do your scanning late at night, when most businesses are closed. Put all your scans in one big notebook, and attempt to scan as much of the Network [the whole phone system if you were wondering] as you can. Another good prefix to scan are the pay <900>/200-XXXX numbers. These generally cost more than most of the normal 900 numbers, and some of them are private AT&T numbers. You can also try NPA-NXX-00XX, and NPA-NXX-01XX. But you don't have to be limited to these. Different numbers can be found in different areas. Explore into deep depths of the Networks' insides, and the deeper you go the better things you will find. Currently in my area, the 98xx numbers have a lot of loops in them, such as <216>/661-9898/9. Here's a listing of prefixes for the <800> exchange and the states that the number resides in (a lot of companies set up numbers that can only be reached in the same state, and others have ones that can only be called outside their state). An asterisk to the right indicates that a toll switching office that accepts MF tones has been found in the area code served by that prefix. An asterisk to the left indicates that numbers have been found in that prefix that can be whistled off using 2600. The numbers that should be hacked for blowable numbers have asterisks before and after them like this: *XXX*.

State	800 Prefix	NPA served
-----	----------	----------
Alabama	633	<205>
Alaska	544	<907>
Arizona	528	<602>
Arkansas	643	<501>
California	227	<415>
	421	<213>
	423	<213>
	854	<714>
	824	<916>
	538	<408>
	235	<805>
	344	<209>
	358	<707>
Colorado	525	<303>
	255	<303>
Connecticut	243	<203>
Delaware	441	<302>
District of Columbia	424	<202>
	368	<202> For high volume traffic
Florida	327	<305>
	237	<813>
	874	<904>
Georgia	841	<912>
	*241	<404>
	554	<404>
Hawaii	367	<808>
Idaho	*635	<208>

Illinois	621	<312>	
	323	<312>	
	637	<217>	
	435	<815>	
	447	<309>	
	851	<618>	
Indiana	428	<317>	
	457	<812>	
	348	<219>	
Iowa	553	<319>	
	*247	<515>	
	831	<712>	
Kansas	835	<316>	
	255	<913>	
Kentucky	626	<502>	
	354	<606>	
Louisiana	535	<504>	
	551	<318>	
Maine	341	<207>	
Maryland	368	<301>	
Massachusetts	343	<617>	
	225	<617>	
	628	<413>	
Michigan	253	<616>	
	521	<313>	
	338	<906>	
	517	<248>	
Minnesota	328	<612>	
	533	<507>	
	*346	<218>	
Mississippi	647	<601>	
Missouri	821	<816>	
	325	<314>	
	641	<417>	
Montana	*548*	<406>	
Nebraska	228	<402>	
	445	<308>	
Nevada	*634	<702>	Las Vegas
	648	<702>	Reno
New Hampshire	258	<603>	
New Jersey	257	<609>	
New Mexico	545	<505>	
New York	223	<212>	
	847	<607>	
	221	<212>	
	431	<914>	
	828	<716>	
	645	<516>	
	448	<315>	
	833	<518>	
North Carolina	334	<919>	
	438	<704>	
North Dakota	*437	<701>	
Ohio	321	<216>	
	543	<513>	

	537	<419>
	848	<614>
Oklahoma	654	<405>
	331	<918>
Oregon	*547*	<503>
Pennsylvania	523	<215>
	345	<215>
	458	<814>
	245	<412>
	233	<717>
Puerto Rico	468	<809>
Rhode Island	556	<401>
South Carolina	*845*	<803>
South Dakota	*843*	<605>
Tennessee	251	<615>
	238	<901>
Texas	527	<214>
	433	<817>
	531	<512>
	231	<713>
	351	<915>
	858	<806>
Utah	453	<801>
Vermont	*451	<802>
Virginia	446	<804>
	368	Arlington - (for D.C.)
	336	<703>
Virgin Islands	524	<809>
Washington	426	<206>
	541	<509>
West Virginia	624	<304>
Wisconsin	*356	<608>
	558	<414>
Wyoming	443	<307>

Another area to scan are the <NPA>/NXX-4499 numbers. These will connect you to a loud annoying busy signal. But the neat part about it is that if anyone else calls it while you're on, you can talk. Many people (I've seen it where they've gotten 20) can be on it at the same time. And the more people on the line, the quieter the busy signal gets. Although the busy signal is annoying, it's good because you don't get charged for busy signals so you can call it direct. Two working numbers are <603>/353-4499 and <205>/356-4499. There are a lot of these, at least one in every area code.

[Detecting Bugs on Home Phones]

FIRST OF ALL TO TEST FOR BUGS, YOU NEED A VOM (MULTIMETER) THE HIGHER THE IMPEDANCE THE BETTER (A DIGITAL WITH FET CIRCUITRY OR A VACUUM TUBE VOLT METER IS THE BEST).

FIRST DISCONNECT THE PHONE LINE(S) AT BOTH ENDS. UNDO THE PHONE INSTRUMENT AND HOOK IT UP TO THE ENTRY POINT OF THE PHONE LINE FROM THE OUTSIDE WORLD (MA BELL DOES NOT LIKE YOU CUT HER OFF COMPLETELY.) THE SCHEME IS THE PHYSICALLY ISOLATE YOUR HOUSE, APARTMENT, FROM THE OUTSIDE WORLD. BUT BEFORE YOU DO THIS MEASURE THE LINE VOLTAGE (IT SHOULD BE APPROXIMATELY 48 VOLTS).

NOW WITH THE WIRES DISCONNECTED AT BOTH ENDS SET YOUR RESISTANCE SCALE TO A HIGH READING AND MEASURE THE RESISTANCE OF THE PHONE LINE, IT SHOULD BE VERY HIGH ON THE ORDER OF MILLION OHMS OR MORE, THIS IS THE NORMAL CONDITION, SINCE YOU ARE MEASURING THE RESISTANCE OF AN OPEN CIRCUIT. IF IT IS MUCH LESS, SAY 50-100KOHMS THEN YOU HAVE A DEVICE ON THE LINE THAT DOES NOT BELONG THERE, PROBABLY A PARALLEL BUG.

NOW TWIST THE END OF THE DISCONNECTED WIRE AND GO TO THE OTHER END AND MEASURE THE RESISTANCE OF THIS. THIS RESISTANCE SHOULD BE ABOUT ONE OHM OR TWO AT THE MOST IN A BIG HOUSE WITH A LOT OF PHONES. IF IT IS MORE, THEN YOU PROBABLY HAVE A SERIES BUG.

IF IN THE FIRST CASE, TAKING PARALLEL MEASUREMENTS USING A METER (NOT LED/LCD) AND YOU NOTICE A "KICK" IN THE NEEDLE, YOU PROBABLY HAVE A LINE TAP

NOW IF YOU ALSO MAKE A MEASUREMENT WITH THE WIRE END TWISTED TOGETHER AND YOU NOTICE THE RESISTANCE READS ABOUT 1-2KOHMS, THEN YOU MAY HAVE A DROP-OUT RELAY. A DROP-OUT RELAY IS A RELAY THAT SENSES A PHONE GOING OFF HOOK, AND SIGNALS A TAPE RECORDER TO START RECORDING.

ANOTHER TEST TO DO WITH THE PHONES STIL HOOKED UP TO THE OUTSIDE WORLD, ON HOOK VOLTAGE IS ABOUT 48 VOLTS AND OFF HOOK IS ABOUT 6-10 VOLTS. ANY OTHER CONDITIONS MAY MEAN TELEPHONE SURVEILLANCE

IF YOU USE A WIDE RANGE AUDIO FREQUENCY GENERATOR AND CALL YOU HOUSE, APARTMENT ETC. FROM ANOTHER PHONE AND SWEEP UP AN DOWN TE SPECTRUM, AND YOU NOTICE THE PHONE ANSWERS ITSELF SOMEWHERE IN THE SWEEP YOU PROBABLY HAVE AN INFINITY TRANSMITTER ON YOUR LINE.

THE ABOVE INFORMATION TELLS NOTHING BUT TELCO TAPS AT THE CENTRAL OFFICE, OR ANYWHERE ELSE ALONG THE LINE, BUT THIS INFORMATION MAY TELL YOU THAT YOUR WIFE, GIRLFRIEND(BOYFRIEND), OR BUSINES ASSOCIATE MAY BE MONITORING YOUR PHONE ACTIVITIES.

AN INFINITY TRANSMITTER,IS A NEAT DEVICE IT ALLOWS YOU TO CALL THE BUGGED PLACE
AND IT SHUTS OFF THE RINGER AND DEFEATS THE SWITCHHOOK, SO THE MOUTHPIECE NOW
BECOMES A ROOM BUG. IT WAS ORGINALLY SOLD FROM THE TRAVELLING BUSINESS MAN
TO MAKE SURE HIS WIFE WAS SAFE AT HOME NOT BEING ATTAKCED...

= Using Diverters =

What Diverters Are:

Diverters, originally knows as "Chesse Boxes" were used in the sixties by bookies and other illegal businesses to forward their calls. Diverters pre-date call forwarding and simulate this custom calling feature with one major advantage. Unlike call forwarding, a diverted call may be intercepted while the phone rings or during conversation just by picking up the phone at the diverter location. After diverters became popular in the crime sector, they became a good way for professionals to recieve night time office calls at home. For this reason may diverters are only up at night.

Locating Diverters:
----

1 - You can recognize a diverter fairly easily. A diverter will ring usually one of two times then you may hear a tone, a moment of silence or a voice saying something like "Please hold you call is being transferred". On some diverters, there is no time laps before the second symptom. The second symptom is another ring... sometimes of a different type. Finally and fatally, if you wait after the person hangs up you will usually hear the diverter dial-tone within a few seconds.

2 - Diverters often belong to:

A: Physicians
B: Dentists
C: Real Estate Offices
D: Financial Advisers
E: 24 Hour Air Cond. Repair
F: 24 Hour Exterminators
G: 24 Hour Heater Repair
H: Insurance Agents
I: Wreckers
J: Anyone Else Of A 24 Hour Nature

How A Diverter Works:

Simply put, a diverter is a small box connected to two phones. When phone #1 rings, the diverter picks up phone #2 dials a number on it and patches the two phones together.

Flaws To A Diverter:

The most commonly known flaw is that if you hold on the line after being hung up on you will usually hear the diverter dial-tone and you can usually dial off of it. This is because you have not hung up on phone #1 and it is still connected to phone #2.

Another flaw is even better. If one person rings phone #2, and another calls phone #1 the two parties will be connected. If either party hangs up, the other will get a dial-tone belonging to the other phone (usually).

Often you will have to hit your "1" key. This simulates a dial-tone and fools the diverter into thinking that the phone is hung up.

You can also sit ringing phone #2 and intercept their calls. One diverter I found belonged to a mail order place and I intercepted calls, obtained credit card numbers, then placed the orders myself so that noone would know what happened.

The History Of British Phreaking

In Britain, phreaking goes back to the early fifties, when the technique of 'Toll A drop back' was discovered. Toll A was an exchange near St. Pauls which routed calls between London and nearby non-London exchanges. The trick was to dial an unallocated number, and then depress the reciever-rest for 1/2 second. This flashing initiated the 'clear forward' signal, leaving the caller with an open line into the Toll A exchange. He could thjen dial 018, which forwarded him to the trunk exchange- at that time, the first long distance exchange in Britain- and foll ow it with the code for the distant exchange to which he would be connect ed at no extra charge.

The signals needed to control the UK network today were published in the "Institution of Post Office Engineers Journal" and reprinted in the Sunday Times (15 Oct. 1972).

The signalling system they use: signalling system No. 3 uses pairs of frequencies selected from 6 tones separated by 120Hz. With that info, the phreaks made "Bleepers" or as they are called here in the U.S. "Blue Box", but they do utilize different MF tones then the U.S., thus, your U.S. blue box that you smuggled into the UK will not work, unless you change the frequencies.

In the early seventies, a simpler system based on different numbers of pulses with the same frequency (2280Hz) was used. For more info on that, try to get ahold of: Atkinson's "Telephony and Systems Technology".

The following are timing and the frequencies for boxing in the UK and other foreign countries. Special thanks to Peter McIvers for the phollowing inpho:

British "bleeper" boxes have the vaery same layout as U.S. blue boxes. The frequencies are different, though. They use two sets of frequencies, forward and backward. Forward signals are sent out by the bleeper box; the backward signals may be ignored (it's sort of like using full duplex). The frequencies are as follows:

U.S.:

US:	700	900	1100	1300	1500	1700
Forward:	1380	1500	1620	1740	1860	1980 Hz
Backward:	1140	1020	900	780	660	540 Hz

for example, change the 900 Hz potentiometers in your box to 1500 Hz. All numbers 1-0 (10) are in the same order as in an American box. The ones after this are thier codes for operator 11, operator 12, spare 13, spare 14, and 15. One of these is KP, one (probably 15) is Star; it won't be too hard to figure out. The signals should carry -11.5dBm +/- 1dB onto the line; the frequencies should be within +/- 4Hz (as is the British equipment). Also, the 1VF system is still in operation in parts of the U.K. This would encode all signals 1 to 16 as binary numbers; for instance, a five is 0101. There are six intervals per digit, each 50ms long r a total of 300ms. First is a start pulse of 2280 for 50ms. Then, using the example of five (0101), there is a 50ms pause, a 50ms pulse of 2280, a 50ms pause, and a 50ms pulse of 2280. Finally, there is a 50ms pause that signals the end of the digit. The frequency tolerance on the 2280 Hz is +/- 0.3%; it is sent at -6 +/- 1dBm. An idle line is signaled by the presence of a 3825Hz tone for more than 650ms. This must be within 4Hz.

France uses the same box codes as the US, with an additional 1900Hz acknowledgement signal, at -8.7 +/- 1dBm per frequency.

Spain uses a 2 out of 5 mf code (same frequencies as US), with a 1700 Hz acknowledge signal.

Other places using the 1VF system are:
Australia, 2280Hz +/-6Hz, 35ms/digit at -6dB.
Germany, France: same as Australia; also, some 1VF systems in the UK.
Switzerland: same as Australia, only it uses 3000Hz, not 2280.
Sweeden: same as above, but at 2400Hz.
Spain: some parts use 1VF with 2500Hz.

There is one other major system: the 2VF system. In this system, each digit is 35ms long. The number is encoded in binary as with the 1VF system. Using the example of five (0101), here's how the American 2VF system was sent:
2400 pulse, pause, 2040 pulse, pause, 2400 pulse, pause, 2040 pulse, pause. The digits and pauses are all 35ms long, for a total of 280ms per digit. Other countries are still using a similar high/low pair with the same timings. Some parts of Italy use the 1VF system with 2040Hz; some use the 2VF system with 2040 and 2400 (same as original US) Hz. The Netherlands uses a 2VF system with 2400 and 2500 Hz pulses. With the 2VF system, all frequencies should be within 2Hz.

Also, here are some specs for American phone equipment:
Dial Tone: 350+440Hz, -17.5 to -14.5 dBm/tone.
Off-Hook (ROH): 1400+2060+2450+2600(!) on/off 5 times per second
Busy: 480+620Hz; solow busy: 0.5 +/- 0.05 sec = 1 period
(about twice a second), at -28.5 to -22.5 dBm/tone.

Ring: 440+480 Hz at -23.5 to -20.5 dBm/tone.
A ring is modulated at 20 +/- 3Hz, 2sec on, 4sec off.

Call waiting: 440Hz, on 1 second.

Recorder Connection: 1400Hz, beeps every 15minutes.
Multiparty line ring: sam% frequency and modulation as ring, but 1sec on, 2sec off (twice as fast).

Now, back to British Phreaking:In the early days of British phreaking, the Cambridge University Titan Computer was used to record and circulate numbers found by the exhaustive dialing of local networks. These number s were used to create a chain of links from local exchange to local exchange across the country, bypassing the trunk circuits. Because the internal routing codes in the UK network are not the same as those dialed by the caller, the phreaks had to discover them by 'probe and listen' techniques or more commonly known in the U.S.--SCANNING. What they did was put in likely signals and listened to find out if they succeeded. The results of scanning were circulated to other phreaks. Discovering each other took time at first, but evenutally the phreaks became organized. The "TAP" of Britain was called "Undercurrents" which enabled British phreaks to share the info on new numbers, equipment etc.

To understand what the British british phreaks did, think of the phone netowrk in three layers of lines: Local, trunk, and international. In the UK, Subcriber Trunk Dialing (STD), is the mechanism which takes a call from the local lines and (legitimately) elevates it to a trunk or international level. The UK phreaks figured that a call at trunk level can be routed through any number of exchanges, provided that the right routing codes were found and used correctly. They also had to discover how to get from local to trunk level either without being charged (which they did with a bleeper box) or without using (STD). Chaining has already been mentioned but it requires long strings of digits and speech gets more and more faint as the chain grows, just like it does when you stack trunks back and forth accross the U.S. The way the security reps snagged the phreaks was to put a simple 'printermeter' or as we call it: a pen register on the suspects line, which shows every digit dialed from the subscribers line.

The British prefer to get onto the trunks rather than chaining. One way was to discover where local calls use the trunks between neighboring exchanges, start a call and stay on the trunk instead of returning to the local level on reaching the distant switch. This again required exhaustive dialing and made more work for Titan; it also revealed 'fiddles', which were inserted by Post Office Engineers. What fiddling means is that the engineers rewired the exchanges for thier own benefit. The equipment is modified to give access to a trunk with out being charged, an operation which is pretty easy in Step by Step (SXS) electromechanical exchanges, which were installed in Britain even in the 1970s (NOTE: I know of a back door into the Canadian system on a 4A CO., so if you are on SXS or a 4A, try scanning 3 digit exchanges, ie: dial 999,998,997 etc. and listen for the beep-kerchink, if there are no 3 digit codes which allow direct access to a tandem in your local exchange and bypasses the AMA so you won't be billed, not have to blast 2600 every time you wish to box a call.

A famous British 'fiddler' revealed in the early 1970s worked by dialing 173. The caller then added the trunk code of 1 and the subscribers local number. At that time, most engineering test services began with 17X, so the engineers could hide thier fiddles in the nest of service wires. When security reps started searching, the fiddles were concealed by tones signalling: 'number unobtainalbe' or 'equipment engaged' which switched off after a delay. The necessary relays are small and easily hidden.

$There was another side to phreaking In the UK in the sixties. Before STD was widespread, many 'ordinary' people were driven to occasional phreaking from sheer frustration at the inefficient operator controlled trunk system.
This came to a head during a strike about 1961 when operators could not be reached. Nothing complicated was needed. Many operators had been in the habit of repeating the codes as they dialled the requested numbers so people soon learnt the numbers they called frequently. The only 'trick' was to know which exchanges could be dialled through to pass on the trunk number. Callers also needed a pretty quiet place to do it, since timing relative to clicks was important

The most famous trial of British phreaks was called the Old Baily trial. Which started on 3 Oct. 1973. What they phreaks did was to dial a spare number at a local call rate but involving a trunk to another exchange Then they send a 'clear forward' to thier local exchange, indicating to it that the call is finished;but the distant exchange doesn't realize because the caller's phone is still Off the hook. They now have an open line into the distant trunk exchange and sends to it a 'seize' signal: '1' which puts him onto its outgoing lines.
Now, if they know the codes, the world is open to them. All other exchanges trust his local exchange to handle the billing; they just interpret the tones they hear. Mean while, the local exchange collects only for a local call. The investigators discovered the phreaks holding a conference somewhere in England surrounded by various phone equipment and bleeper boxes, also printouts listing 'secret' Post Office codes. (They probably got them from trashing?) The judge said: "some take to heroin, some take to telephones" for them phone phreaking was not a crime but a hobby to be shared with phellow enthusists and discussed with the Post Office openly over dinner and by mail. Their approach and attitude to the worlds larges computer, the global telephone system, was that of scientist s conducting experiments or programmers and engineers testing programs and systems. The judge apeared to agree, and even asked them for phreaking codes to use from his local exchange!!!

FAX MACHINE FUN

INTRO-

In the late 80's we have seen a massive explosion in the popularity of fax machines. Everyone has one. They are cheap, easy to use, and very usefull. Up untill now, however, they have been almost exclusivly in the province of the buisness world
. Just for those of you who have been in comas for the last few years, I'll explain fax machines to you.

Fax machines are combination scanners/modems/printers. You can transmit the contents of a piece of paper to another fax over the phone lines. Usually, your fax also prints the number you called from on the first sheet of the transmittal. It is easy to see why buisnesses like these. No longer content with Federal Express, now letters can go cross country in minutes. Faxes have about 200-250 dpi resolution, and print out on rolls of thermal paper. For some odd reason, most of them are 4800 baud.

THE GOOD PART-

"So what" you ask? Most people don't seem to realize the potential available here. When I worked at The FHLB, we used to get faxes all the time, with requests for checks. Occaisionaly, we also got short notes from the idiots at the other banks.
This is what gave me the idea for what I call, for lack of a better term, Fax Piracy.

Fax Piracy is the ultimate crank call. Let me give you an example.

There was this Library I hated, and, like everyone else, they have a fax. So what me and a few of my freinds did was send them requests, "from" another Library for books. I found out later, from a kid who worked there that they wasted about $50, sending them all the books. Not much, but if you know how cheap librarians are, you can imagine the shit fits they had.

Next, we send them a "Mobius Fax" we got some sheets of black construction paper, taped about 10 of them together, and started feeding them through the fax. Once the start of the long sheet we had created came through, we taped it to the end.

This went on continuosly for about 15 minutes untill their (very expensive) thermal paper ran out. Since we had sent them nothing but black paper, it completely covered and ruined all of their paper. This used up their 3month paper allocation at once, and they had to borrow from petty cash to buy more.

Finally we sent them a little note, telling them what idiots they were, and signing it "the fax pirates"

HOW TO DO IT-

First, and this is VERY IMPORTANT- Always remember to REPROGRAM the fax so it displays someone elses name and number. If you forget to do this, its like sending a letter bomb with a return adress.

Second, decide what to send. This is entirely up to you (duh) , and depends on whether you want to annoy them, or really destroy them.* Wierd requests from other campies you hate, long rambling stories, or strange art is always good. Be a little creative. (this part is especially fun if you have a Mac, and access to a laserwriter)

Third, send it. (wow, some people need to be told everything, don't they)
What? You don't know their fax #? Its not in information? Its not in the phone book? Well, keep reading!

HOW TO GET FAX PHONE NUMBERS-

This is just way easier than it should be. Call and ask. I'm serious, we've done this probably over 30 times, and NO ONE HAS EVER QUESTIONED OUR REQUEST! I'll give you a sample of a call that actually happened. (this is verbatum)(we taped it)

IBM LADY Hello, IBM, may I help you?

ME Hi, this is Biff Fulgate from over here at Linear Data Systems Can I get your fax number, those boys in research need to send something over and they lost the number again.

IBM LADY Please hold on a moment

ME Sure thing. Hah, those cooks over in research would probably lose their heads if they wern't screwed on.

IBM LADY Haha. Now is that the Tower 700 number?

ME Um...let me check here... Yeah, that's it. (Tower 700? what?)

IBM LADY Ok, hold on

(Long wait during which I get slightly nervous)

IBM LADY Ok That number is 313-xxx-xxxx

ME Thanks, Bye

Also, most ads have fax numbers. Don't fuck with little companies though. A) they don't need it, B) they are probably more suspicious, C) it hurts them more than it would hurt a big company. be a caring capitolist.

If you need any suggestions as to who's number to get try the following- newspapers, radios stations, big companies, libraries, city & state governments, the right to life movement, ect.

HINTS-

Act like you know whats going on at all times.
Be polite, and a little bit familiar
Make sure you have a plausable reason for getting the number
Don't laugh
Let the person who sounds most 'adult-like' make the call
Make sure you have a plausable name

Remember, the larger the company, the less the people know and care about other parts of the company, so the greater chance you have of not getting hassled.
ALSO! Don't forget to change the "number" you are calling from.

If you want to send a Mobius Fax, usually Faxes have paper feed trays (we didn't know that when we did it)

ALSO- NEVER, EVER, DO THIS TO ATT!

HOW TO GET A FAX TO USE-

Well, if you don't have one, try mommy's or daddy's office. Most Campus offices have faxes you can pretend that you are supposed to be using (tell them the Library sent you). Many print-shops (like Kinko's) have fax machines that you can use for
a nominal fee. And, just like terminals in the early 80's, most fax machines are just sitting out in offices, if you dress nicely, and look like you know what you're doing, no one is going to ask questions.

FAX INTERCEPTION

This article is reprinted from Full Disclosure #23. Copyright (c) 1991 Full Disclosure. Permission granted by publisher to reprint when subscription information provided: Full Disclosure, Box 903-R, Libertyville, Illinois 60048, Phone: (708) 395-6200, Fax: (708) 395-6022, BBS: (708) 395-3244, Toll free: (800) 786-6184. Subscriptions: $18 for 12 issues.

As with the introduction of all new communications technologies, there is a time lag between the availability of the technology and commercial development of interception devices. Accompanying the use of both are unanticipated risks and the potential for misuse and misunderstandings.

False Sense of Security

With the widespread proliferation of fax machines came increased use. In general, a document transferred has been given the same sort of validity as one sent or received by U.S. Mail. In general, such communications were originally secure. Now that interception equipment is available, the sense of security has become false.

For all practical purposes, fax is a remote photocopying machine. The process begins with the sending unit converting the image on the page into a digitized image (numbers in an electronic format) and transmitting it as a noise sounding signal over a phone line. The receiving fax converts the signal into dots and prints it.

Since the image is transmitted over standard phone lines, the communication is subject to interception. However, rather than tapping the line with a tape recorder or simply listening to the oral communications, an interception device that makes sense of the specialized signal is necessary. Sometimes this is done by recording the transmission and later converting the recording of the modem signal to a computer image, sometimes it is done 'on the fly' as the signal is being intercepted.

Simple Fax Intercepts

Why not just use a standard fax machine for interception? The signal sequences and handshaking at the time machines first connect complicates the possibility. During startup, the machines automatically select one of several built in protocols depending on line conditions. That is why on really noisy connections, the transmission of a page can take much longer. Directly connecting a 3rd fax machine to the line may confuse this process. Both the receiving unit and the intercepting machine would be sending signals about line conditions and protocol. However, if a 3rd fax machine did manage to get properly synchronized to the signal in use without interfering with the initial handshake, it would print an image identical to the one received by the intended recipient. We had mixed results when we tried this in our lab. Sometimes we managed to get all three machines synchronized. Using unmodified fax machines to attempt intercepts didn't provide sufficient reliability to be considered a viable approach. Indeed, continued attempts of this approach would likely put both sender and recipient(s) on notice that something was wrong as connections would be repeatedly lost.

This doesn't mean that it is really complicated to intercept faxes. The Philadelphia Inquirer reported in September 1990 that Japanese hackers have been stealing valuable information from corporations by using fax interception. The article claimed it could be done by anyone with a little knowledge of electronics. We agree, we have intercepted faxes in our lab. (See front cover for one such example.)

Doing It Right

The latest commercially available fax interception devices generally use fax boards in IBM PC or compatible computers. The actual hardware used for fax interception is often the same as used by normal computer-fax systems. The software is more sophisticated. Rather than attempting to synchronize with the sending unit by sending protocol information, it adjusts to whatever protocol the two main players have established and stores the signal information.

After interception, the electronic information is stored in the computer and is available for review, to be printed, altered or discarded. Such equipment can be left unattended for long periods if necessary, or monitored for the instant use of information in cases where law enforcement is standing by waiting for some specific bit evidence.

Cellular Fax Interception

Cellular phone based fax machines provide ripe opportunity for `hacker' intercepts, since the signal is available via low cost police scanners. No physical connection to a common carrier network is necessary. There is absolutely no risk of being detected.

Commercial fax interception equipment gets more complicated, though. Since fax messages might be on the same phone lines as voice or other computer modem communications, some of the interception devices automatically route different types of communications to different interception devices. This provides the interceptor with a separate recordings of voice phone calls, faxes, and other computer communications.

Such fax interceptions are based upon the interceptor having a specific target. Distributing the sorts of information received for analysis isn't much different from an ordinary, now old fashioned, wiretap.

Broadband Interception

Presorting of signals and voice communications as described above makes broadband scanning for fax messages easy. The interception of satellite or microwave links has become possibile. Cooperation by a common carrier with the government has happened in the past, and strikes a chord of dangerous reality today. But it really takes little by way of home fabricated equipment to monitor much of the satellite link traffic. Commercial equipment is also available. One commercial fax interception unit can decode up to 150 simultaneous fax transmissions from a 6,000 phone line satellite link.

Such broadband interception can also be done on oral calls, however, the task of listening to all the conversations for the important ones is much, much greater compared to scanning faxes. First, faxes are usually much more direct and to the point than normal phone conversations (not so much about Sunday's game). Additionally, optical character recognition (OCR) process can be used to convert much of the text to standard computer data and then be mechanistically selected for closer scrutiny by an automated search of keywords of interest. Encryption of a fax could also be noted, perhaps triggering further attention.

The risks resulting from broadband interceptions are henious. Your fax could be intercepted not because you were a selected target of law enforcement, industrial spies or miscreant hackers, but because of the route your fax travelled through the common carrier networks. Broadband interceptions become a modern day version of general warrants. Satellite signals don't respect borders. Interception in nations with no privacy concerns for radio signals of what we, as users, understand to be Constitutionally protected communications has become a real threat. There are areas contained within our national frontiers where the United States Constitution does not apply. Foreign embassies present one such clearcut example. The status on Indian Reservations is not cleancut.

Dangers of Fax

The February 13, 1990 issue of the American Bankers' Association publication ``Bankers Weekly'' reported that ``In one incident, a bank suffered a $1.2 million loss through fraudulent funds transfer requests which were accomplished using nothing more than business letterhead, tape and sissors.'' A fax machine made such simple tools effective. Inordinate reliance on technology permitted the loss to actually happen.

The journal continues that there is a need for legislation (changes to the Uniform Commercial Code) to put a stop to the problem. Unfortunately, legislative efforts alone cannot correct the problem. The first step, is an understanding of the technology.

Once the technology is understood, administrative procedures can be implemented by users of fax machines to protect themselves. That protection cannot be successful without understanding the limitations of the machinery. Taking any communications device for granted is a high risk path.

New Techniques For Fraud

The advent of fax technology has opened the door to new methods of fraud. Those intent on committing fraud have always devised methods of bypassing normal authentication systems in order to steal. As technology evolves, these methods also evolve. Protective measures must follow suit.

Faxes represent a multiple whammy. People who send faxes have some geographic distance between them. Because of past reliance on semi-automated communications, formal verification proceedures are bypassed, substituting the mysterious nature of modern communications. There was a time, even recently, that tellers at banks asked for positive identification even in the case of small cash transactions inside a bank. Yet today we witness orders for large sums being processed simply because ``it came by fax." This is truly a conspiracy of laxness and misinformation.

A written purchase order from a company is likely to have a particular form, and include a signature. One attempting to issue a fraudulent purchase order would need to forge both the form and the signature. Additionally, envelopes and possibly a postage meter imprint from the issuing company would also be needed. Elsewhere in this issue we reprint a letter from the Federal Communications Commission. The letterhead was, for reasons we have been unable to determine, typed instead of printed. Some of the recipients we've talked to have placed calls to verify the authenticity of the letter. As it turns out, the letter was authentic and official.

A purchase order sent by fax on the other hand, can be created by cutting, pasting and xeroxing together parts of other orders from the company. When received by fax, the fake would appear legitimate.

PC's & Fax: The Miscreants Gun

The advent of PC based fax boards exaggerates these problem. A fax that originates, is received by, or intercepted by a personal computer (PC) fax board really opens the door for miscreants.

A fax, when stored on a PC is easily modified using ordinary commercial software intended for preparation of graphics. An image of the fax can be brought up on the screen and parts of it altered or cut and pasted electronically. For example, a purchase order could have a shipping address altered. A signature could be removed from one document and placed on another. All such operations can be done on a computer screen in moments. Document changes that could take a professional forger hours to accomplish could be done in minutes by an amateur, even an underage one.

Bogus faxes can be created to be sent to another fax, or incoming faxes could be altered by an employee and printed as authentic. Detection is difficult to impossible, depending on verification techniques used at audit.

The difficulty of intercepting standard U.S. Mail or voice phone calls and altering the content by a third party is enormous compared to fax messages. Before a fax message is printed, it is just a series of electrical signals. Any alternations result in changes without a trace of the alteration.

The receipt of a fax is <B>not<D> a confirmation of its content, unless other corroborative authentication validates the information.

Someone with access to a phone closet can route incoming fax line to a PC. The fax can then be connected to a different phone line. All incoming faxes would be first received by the PC and the operator could alter, erase, or forward without change those faxes to the standard fax machine. A pre-review and alteration if desired scheme can be effected. The same can not easily be accomplished with normal voice phone calls, or the U.S. Mail.

With the advent of the Caller-ID services, this information should soon be incorporated into fax machines, so the true number of the caller will be placed on the fax. This will still do nothing to prevent transmission of bogus faxes over that phone line.

Protect Yourself

The best rule for protecting one's interests when using faxes is to use them only with other confirmation or as confirmation of other communications. They should never be used for final copies of contracts, purchase orders or other important documents that could have a significant impact if altered, or entirely fabricated. Where would we be if our WW2 treaties terminating hostilities were faxed documents. Additionally, information that would not be given out over a standard phone conversation, subject to a wiretap, or other listeners (via a speakerphone, extension, etc), should not be sent by fax. There is no way to tell who may pick up a received fax and read it. In fact, it is more likely an unintended party will read a fax than pick up an extension phone and eavesdrop on a voice call (intentionally or not).

It should be kept in mind that any errant employees or others that could get access to the fax phone line(s) could intercept all faxes sent or received and make use of the fax images for whatever purpose they desired.

The intercepted faxes can be used to collect or create incriminating evidence, industrial espionage, or as the base of documents to be used in forgery. There's a whole new meaning to autograph collection.

Conclusion

Fax technology in its current form provides a useful service for business and others. However, the risks must be examined so the use doesn't go beyond that which is appropriate given its current functionality / risk ratio.

In conclusion, the convenience of a fax must be weighed against its risks and procedures implemented to authenticate incoming and outgoing faxes as well as what information is communicated by fax. As with all technologies, it must be understood so that it can be used for purposes that are appropriate for the needs of the technology and the user. A lack of understanding can leave the user exposed to unnecessary danger, liability and loss. When used with an understanding of the benefits as well as the pitfalls, a fax machine can greatly enhance productivity.

Subject: Public FAX Machines/Phraud

pay fax machines in public libraries and similar places, and some people in the BBS community discovered a number of methods of phraud based upon these machines. Some of these machines contain an automatic dialer that automatically calls an 800 number, where an operator picks up the phone and asks for your credit card number, verifies it, and connects you to your destination fax machine, running the call through. I don't know exactly how answer supervision is handled here, but using fax machines, one could use the carrier tone.

I discovered that, when the machine was unplugged, one could pick up the handset and get a regular dial tone. There is no touch-tone pad, so it's impossible to dial out normally, but one can dial by clicking the switchhook, and bopping the switchhook ten times connects you to an operator, and you can give her the phone number that you want to dial. I used this to make a local call just to see if this could be done, and I mentioned this to a friend.

Other people in the BBS community in that area later discovered that there was no toll restriction on those lines, either, so one could dial two zeros, get an AT&T operator, and then call his phriends anywhere in the world. A person armed with a tone dialer would have a whole spectrum of phraudulent options availible to him -- the 'start a conference and transfer control to a pay phone' trick, never mind just calling 900 numbers with a tone dialer just for the hell of it.

Of course, I can't advocate any of this behavior because it is illegal or immoral, but public fax machines, like COCOTS, have some weaknesses against phraud -- and they really could design them quite a bit better so they both provide better service and are more resistant to people with evil intent.

[Moderator's Note: The public Fax machine that was installed in the post office downtown was a sham, security-wise. They had the phone line plugged into a modular jack mounted on the wall next to it. By unplugging the Fax machine and plugging in an ordinary phone, you got dial tone that would get you anywhere. And no one at the post office seemed to keep an eye on the machine or care who did what over in that corner of the (relatively, in the wee hours of the morning) deserted lobby area. The machine was removed a couple months ago and the phone line -- I assume -- turned off ... but who knows.

GOLD BOX PLANS: HOW TO BUILD IT

YOU WILL NEED THE FOLLOWING:

TWO 10K OHM AND THREE 1.4K OHM RESISTOR ES, TWO 2N3904 TRANSISTORS, TWO

PHOTOCE LLS, TWO RED LED'S (THE MORE LIGHT PROD UCED THE BETTER), A BOX THAT WILL NOT L ET LIGHT IN, AND RED AND GREEN WIRE.

LIGHT FROM THE #1 LED MUST SHING DIREC TLY ON THE PHOTOCELL #1. THE GOLD BOX I MAID NEEDED THE TOP OF THE LED'S TO TOU CH THE PHOTOCELL FOR IT TO WORK. THE SAME APPLIES TO THE #2 PHOTOCELL AND LED 1

```
   :-PHOTOCELL--:
   :           :
   :           :BASE
   :   1     TTTTT
   :  +LED-   TRANSISTOR
   :         TTTTT
   :          : :
   :  -I(--    : :COLLECTOR
RED1--<     >:--: :-------:-----GREEN2
      -I(-- :           ----------:
           :                    :
       2    :-/+/+/-/+/+/-/+/+/-/+/+/
      LED     10K    10K   1.4K 1.4K
               RESISTORES
```

```
          2
      -PHOTOCELL-----------------
      :                      :
      :BASE                  :
    TTTTT                     :
    TRANSISTOR                 :
    TTTTT                     :
     : :EMITTER               :
GREEN1- --------------------------RED2
    :   :
    /+/+/
     1.4K
```

THE 1.4K RESISTOR IS VERIABLE AND IF TH E SECCOND PART OF THE GOLD BOX IS SKIPPE D IT WILL STILL WORK BUT WHEN SOMEONE P ICKS THE PHONE UP THEY WILL HEAR A FAIN T DIAL TONE IN THE BACKGROUND AND MIGHT REPORT IT TO THE GESTOPO ER...(AT&T). 1.4K WILL GIVE YOU GOOD RECEPTION WITH LITTLE RISK OF A GESTOPO AGENT AT YOUR DOOR.

NOW THAT YOU HAVE BUILT IT TAKE TWO GREEN WIRES OF THE SAME LENTH STRIP THE ENDS, TWIST TWO ENDS TOGETHER AND CONN ECT THEM TO GREEN1 AND PLACE A PEICE OF TAPE ON IT WITH LINE #1 WRITING ON IT. CONTINUE THE PROCESS WITH RED1 ONLY US E RED WIRE. REPEAT WITH RED2 AND GREEN2 BUT CHANGE TO LINE #2.

HOW TO INSTALL
____

YOU WILL NEED TO FIND TWO PHONE LINES THAT ARE CLOSE TOGETHER. LABEL ONE OF THE PHONES LINES LINE #1.CUT THE PHONE LINES AND TAKE THE OUTER COUTING OFF I T. THERE SHOULD BE 4 WIRES CUT THE YELL OW AND BLACK WIRES

OFF AND STRIP THE RE D AND GREEN WIRES FOR BOTH LINES.

LINE #1 SHOULD BE IN TWO PEICES TAKE THE GREEN WIRE OF ONE END AND CONNECT IT TO THE ONE OF THE GREEN WIRES ON THE GOLD BOX. TAKE THE OTHER HALF OF LINE # 1 AND HOOK THE FREE GREEN WIRE TO THE G REEN WIRE ON THE PHONE LINE. REPEAT THE PROCESS WITH RED1 AND THE OTHER LINE.

ALL YOU NEED TO DO NOW IS TO RIGHT D OWN THE PHONE NUMBERS OF THE PLACE YOU HOOKED IT UP AT AND GO HOME AND CALL IT. YOU SHOULD GET A DIAL TONE!!! IF NOT LEAVE ME A MESSAGE ON THE MODEM MADNESS BBS 516-569-0589 OR TRY CHANGING THE EMITTER WITH COLLECTOR. OH AND HOOKING IT UP TO A PAYPHONE IS A FEDERAL OFFENCE AND IS ILLEAGAL TO PUT ON ANY PHONE. I RECOMMEND YOU SEE YOU R LOCAL POLICE DEPARTMENT BEFORE DOING ANYTHING SAID IN THIS ARTICLE. (HAHAHAHA!!!!!!)

JACKBOX

MA BELL IS NOT THE ONLY ONE WITH STANDARDS! JUST ABOUT EVERY MANUFACTURER OF IC'S THAT GENERATE TOUCH TONES HAS ALSO GONE BY THE 16 KEY (8 TONE) STANDARD FOR TOUCH TONE PADS. AND IT IS EVEN EASIER TO CONVERT A TONE PAD THAT USES AN INTEGRATED CIRCUIT TO GENERATE THE TONES THAN CONVERTING A MA BELL PAD!

IT WILL HELP IMMENSELY IF YOU HAVE THE SCHEMATIC FOR THE PAD IN QUESTION, OR AT LEAST THE PIN-OUT DIAGRAM OF THE CHIP BEING USED. PIN-OUTS CAN USUALLY BE OBTAINED FROM THE MANUFACTURER OR FROM AN ECG, SK, GE OR SIMILIAR SEMICONDUCTER HANDBOOK (PROVIDED THAT MANUFACTURER MAKES AN EQUIVALENT FOR THE CHIP IN YOUR PAD). I'LL USE THE RADIO SHACK CEX-4000 TONE PAD MODULE FOR AN EXAMPLE, EVEN THOUGH IT IS PROBABLY ALMOST THE LOUSIEST ONE YOU CAN BUY, IT IS FAIRLY TYPICAL ASILY AVAILABLE.

TAKE A LOOK AT THE DIAGRAM OR THE PIN-OUT OF THE CHIP. YOU SHOULD SEE TWO GROUPS OF PINS, THE ROWS TONE PINS AND THE COLUMN TONE PINS. THESE WILL BE MARKED AS R1,R2,R3,R4 AND C1,C2,C3 (RADIO SHACK) OR OR X1,X2,X3 AND Y1,Y2,Y3 ETC. ON OTHERS. AT ANY RATEU SHOULD BE ABLE TO DISTINGUISH WHICH THREE PINS CONTROL THE COLUMNS AND WHICH FOUR CONTROL THE ROWS. IF YOU'RE LUCKY, EACH GROUP OF ROWS AND COLUMNS WILL BE CONTIGUOUS. NOW LOOK AT THE COLUMN PINS, AND YOU'LL PROBABLY SEE AN EMPTY PIN RIGHT NEXT TO THEM. THIS IS THE COLUMN PIN FTHE 1633 HZ TONES. THESE CHIPS USUALLY ACHIEVE THEIR SWITCHING BY CONNECTING A ROW PIN WITH A COLUMN PIN (THAT WAY TQAN USE A0VERY SIMPLE KEYBOARD PAD, UNLIKE MA BELL'S COMPLICATED ONE). SO ALL YOU HAVE TO DO IS TAKE A SPDT SWITCH AND A FEW PIECES OF WIRE, CUT THE TRACE GOING TO THE COLUMN 3 PIN OF THE CHIP, ATTACH A WIRE FROM THE CHIP SIDEOF THAT CUT TO ONE END OF THE

SPDT SWITCH, A WIRE FROM THE OTHER SIDE OF THE CUT TO THE CENTER OF THE SPDT SWITCH, AND FINALLY, FROM THE REMAINING CONTACT ON THE SPDT SWITCH, HOOK A WIRE TO THE PREVIOUSLY IDENTIFIED PIN C4 (COLUMN 4). NOW YOU HAVE A "BANK SWITCHING ARRANGEMENT EXACTLY LIKE THE ONE DESCRIBED IN THE PREVIOUS BULLETIN FOR MODIFYING A MA BELL PAD.

IF YOU CAN'T GET THE SCHEMATICS OR THE PIN OUTS FOR YOUR CHIP, DON'T DESPAIR. THERE IS STILL HOPE FOR YOU! YOU JUST HAVE TO TRACK THE CONNECTIONS GOING FROM THE PAD'S KEYS TO THE CHIP. CHANCES ARE YOU'LL FIND THAT EACH ROW HAS A COMMON TRACE, AND SO DOES EACH COLUMN (FOR THOSE NON-TECHNICAL FOLKS, A TRACE IS A CONNECTION ETCHED OUT ON A CIRCUIT BOARD). JUST FOLLOW THESE TO THE CHIP, AND MAKE YOUR OWN SCHEMATIC UP. NOW TAKE A LOOK FOR THAT EXTRA PIN--THERE SHOULD BE ONE FLOATING AROUND RIGHT NEXT TO THE COLUMN PINS. IT WILL BE NOT BE HOOKED UP TO ANYTHING ELSE, THAT IS, "HANGING FREE". DRILL A HOLE IN THE SIDE OF TONEPAD'S CASE, AND MOUNT YOUR SWITCH. RADIO SHACK SELLS A NICE MICROMINIATURE SWITCH

****How to get MONEY from payfones****

Getting money from a payphone requires only a few simple things.
1.Intellegence-You have to know when to do this kind of thing. If you do it in broad daylight, with a bunch of people watching you, you'll have the TELCO on you so fast you won't know what happened
2. You must select a phone that you can have access to its wires. (Look for a plastic shroud running down the wall, or the junction box outside!) On a normal phoneline, only two wires are used:Ring & Tip. (Red & Green). The payphone uses the red and green for its telephone operations, but it also uses the yellow & black to control the coin mech. relays & solenoids. Find a section of the wire where a cut will not be easily seen. Strip off the insulation of the cord, exposing the four wires. Now, get out the all purpose wire cutters (Or finger nail clippers if you like) and cut the black & yellow wires. Now just sit back and let people use the phone!

What Happens? Well, when you put money into a payphone, it stays in the coin mechanism until 1 of 2 things happen.
1. You connect your call, talk, and Hangup. After you hangup, your money goes to the collection box. (The only way to get the money then is to rip the box out!)
2. You call a number that doesn't answer, or get busy signal, or something like that, and then hangup. When you hangup, the money goes from the coin mech. to the coin return.

That is the key! After the Black & Yellow wires have been cut, the money goes neither to the coin box or coin return! It just sits there! All you have to do is come back at like 3:00 in the morning, re-connect the black & Yellow wires, pick up the han dset & put it back down.

**********JACKPOT********** All the money that was put in that phone that day comes shooting out the coin return. (Just like in the movies!) It is the AWESOMEIST FEELING! I have collected upto $30 a day doing this to phones all around town!

Dangers: The people that put money in and don't get connected or get a busy signal and hang up do NOT get their money back. Usually they will call the operator who inturn calls the Repair Dept. (That is why it is important to cut the wire where it can not be seen. But if you want to do this as a one time thing.........GO FOR IT! Oh yes, alternate phones every other couplple of days or so. Stay on your toes and watch out for white Vans!!!!) If someone sees you taking money out of the coin retur n (Getting $15 in change out of a phone is not common!) Just say you hung up the phone and all this mony started pouring out! (It doesn't hurt to give them a little of it either!) After a month or two the Phone Co. catches on, so I do not reccomend usin g one phone for over two weeks.

Telephone Info

BRIDGING HEADS, RESIDENTIAL AND
BUSINESS MULTILINE DISTRIBUTION BOXES,
LINE AND TRUNK SPLITTERS, AND
OTHER BELL SYSTEM WIRE TERMINATIONS.

- HOW TO USE, AND/OR ABUSE THEM -

(INCLUDING A TUTORIAL ON BASIC TELEPHONE EAVESDROPPING TECHNIQUES.)

****

WRITTEN BY : PHUCKED
AGENT
04

****

IN THIS ARTICLE, I WILL FIRST BESCRIBE THE TERMINATION, WIRING, AND TERMINAL HARDWARE MOST COMMONLY USED IN THE BELL SYSTEM, AND I WILL INCLUDE A SECTION ON METHODS OF USING THEM.

****

LOCAL NETWORK

THE LOCAL TELEPHONE NETWORK BETWEEN THE CENTRAL OFFICE/EXCHANGE AND THE TELEPHONE SUBSCRIBERS CAN BE

BREIFLY DESCRIBED AS FOLLOWS:

FROM THE CENTRAL OFFICE (OR LOCAL EXCHANGE) OF A CERTAIN PREFIX (ES), UNDERGROUND AREA FEEDER TRUNKS GO TO EACH AREA THAT HAS THAT PREFIX. (USUALLY MORE THAN ONE PREFIX PER AREA) AT EVERY FEW STREETS OR TRACT AREAS, THE UNDERGROUND CABLES SURFACE. THEY THEN GO TO THE SECONDARY TERMINATION, (THE AERIAL TELEPHONE FEEDER CABLE) (OR BACK UNDERGROUND, DEPENDING ON THE AREA) AND THEN TO THE SUBSRIBERS HOUSE (OR IN THE CASE OF AN APARTMENT BUILDING OR MUTLILINE BUSINESS, TO A SPLITTER OR DISTRIBUTION BOX/PANEL).

****

NOW THAT WE HAVE THE BASICS, I'LL TRY AND GO IN-DEPTH ON THE SUBJECT.

UNDERGROUND CABLES

THESE ARE SOMETIMES INTER-OFFICE TRUNKS, BUT USUALLY IN A RESIDENTIAL AREA THEY ARE FEEDER GROUPS THAT GO OTO BRIDGING HEADS OR DISTRIBUTION CASES. THE CABLES ARE ABOUT 2-3 INCHES THICK (VARIES), AND ARE EITHER IN A METAL OR PVC-TYPE PIPE (OR SIMILAR). RARELY (MAYBE NOT IN SOME REMOTE RURAL AREAS) ARE THE CABLES JUST 'ALONE' IN THE GROUND. INSTEAD, THEY ARE USUALLY IN AN UNDERGROUND CEMENT TUNNEL (RESEMBLES A SMALL SEWER OR STORMDRAIN) . THE MANHOLES ARE >HEAVY< AND WILL SAY 'BELL SYSTEM' ON THEM. THEY CAN BE OPEN ED WITH A 1/2 INCH WIDE CROWBAR (HOOK SIDE) INSERTED IN THE TOP RECTANGULAR HOLE. IF YOU GET IT OPEN, GO INSIDE!! THERE ARE LADDER RUNGS TO HELP YOU CLIMB DOWN. YOU WILL SEE THE CABLE PIPES ON THE WALL, WITH THE BLUE AND WHITE STRIPED ONE BEING THE INTER-OFFICE TRUNK GRP (AT LEAST IN MY AREA). THE OTHERS ARE LOCAL LINES, AND ARE USUALLY MARKED OR COLOR CODED. THERE IS ALMOST ALWAYS A POSTED COLOR CODE CHART ON THE WALL, NOT TO MENTION TELCO MANUALS DESCRIBING THE CABLES AND TERMINALS, SO I NEED NOT GET INTO DETAIL. AGAIN: >IF YOU CAN GET INTO A BELL MANHOLE, DO IT!, IT WILL PAY OFF <. ALSO, THERE IS USUALLY SOME KIND

OF TEST EQUIPMENT, AND OFTEN BELL
TEST SETS ARE LEFT IN THERE.
SO GET YOUR CROWBARS!

****

BRIDGING HEADS - (WE MS2'S)

THE INNOCENT-LOOKING GRAYISH-GREEN BOXES.
WHEN IN GROUPS OF TWO OR THREE, THEY
ARE FOR SECONDAY/TERTIARY TERMINATION
AND ACCESS POINTS (BRIDGED ACCESS).
THESE ARE THE WESTERN ELECTRIC SAI
55 OR 22/E TERMINAL CASES. THEY HOLD
ON THE ORDER OF 900-1200 CABLE PAIRS.
THIS IS USUALLY THE SECOND TERM. POSI
TION ON THE LOCAL LOOP (AFTER THE MTF
FRAME AT THE CO/ OR THE UNDERGROUND
'FTP' POSITION).
THESE CAN BE EITHER
TRUNK BRIDGES OR BRIDGING FOR RESIDEN
CES. THE AREA FEEDER BRIDGING HEADS
ARE USUALLY LARGER, AND THEY HAVE THE
'WESTERN ELECTRIC' LOGO AT THE BOTTOM,
WHEREAS THE NORMAL BRIDGING HEADS
(WHICH MAY BE DIFFERENT IN SOME AREAS-
DEPENDING ON THE COMPANY YOU ARE
SERVED BY. GTE B.H'S LOOK SLIGHTLY
DIFFERENT. ALSO, DO NOT BE FOOLED
BY SPRINKLER BOXES!)
CAN BE FOUND IN JUST ABOUT EVERY CITY.

TO OPEN A BRIDGING HEAD:
IF IT IS LOCKED (AND YOU'RE FEELING
DESTRUCTIVE), PUT A HAMMER OR CROWBAR
(THE SAME ONE YOU USED ON THE MANHOLE
) IN THE SLOT ABOVE THE TOP HINGE OF
THE RIGHT DOOR. PULL HARD, AND THE
DORR WILL RIP OFF. VERY EFFECTIVE!
IF IT ISN'T LOCKED (AS USUAL),
TAKE A 7/16 INCH HEX SOCKET AND
WITH IT, TURN THE BOLT ABOUT 1/8 OF A
TURN TO THE LEFT (YOU SHOULD HEAR
A SPRING RELEASE INSIDE). HOLDING THE
BOLT, TURN THE HANDLE ALL THE WAY TO
THE RIGHT AND PULL OUT.

NOW INSIDE, FIRST CHECK FOR
A TEST-SET (WHICH ARE OFTEN LEFT BY
BELL EMPLOYEES). THERE SHOULD BE A
PANEL OF CABLE PAIRS + SCREW TERMINALS
(TYPE 45/47IB REGULAR BINDERS) . PUSH
THE PANEL BACK ABOUT AN INCH OR SO,
AND ROTATE THE TOP LATCH (ROUND WITH
A FLAT SECTION) DOWNWARD. RELEASE THE

PANEL AND IT WILL FALL ALL THE WAY
FORWARD. THERE IS USUALLY A LARGE AMOUNT
OF WIRE AND EXTRA TERMINALS.
THE TEST-SETS ARE OFTEN HIDDEN HERE,
SO DONT OVERLOOK IT (400 FOOT ROLLS OF
#22 SOLID WIRE ARE OFTEN NEAR THE TOP
IN THE BACK OF THE BOX. 'BORROW THEM')
. ON THE RIGHT DOOR IS A METAL BOX OF
INSULATORS, BINDERS, CLIPS, ETC. TAKE
A FEW (COMPLIMENTS OF BELL...). ON EACH
DOOR IS A USEFUL ROUND METAL DEVICE.
(SAYS 'INSERT GENTLY' OR 'CLAMP GENTLY
 - DO NOT OVERTIGHTEN' ETC..) ON THE
FRONT OF THE DISC, YOU SHOULD FIND TWO
TERMINALS. THESE ARE FOR YOUR TEST SET.
(IF YOU DONT HAVE ONE, DONT DEPAIR -
I'LL SHOW YOU WAYS TO MAKE BASIC TEST
SETS LATER IN THIS ARTICLE).
HOOKING THE RING (-) WIRE TO THE
'R' TERMINAL; AND THE TIP (+) WIRE
TO THE OTHER. (BY THE WAY, AN EASY WAY
TO DETERMINE THE CORRECT POLARITY IS
WITH A 1.5V LED. TAP IT TO THE TERM.
PAIR, IF I DOESNT LIGHT, SWITCH THE
POLES UNTIL IT DOES. WHEN IT LIGHTS,
FIND THE LONGER OF THE TWO LED POLES.
THIS ONE WILL BE ON THE TIP WIRE (+))
 BEHIND THE DISC IS A COILED UP CORD.
THIS SHOULD HAVE A SPECIALIZED CONNECTOR.
ITS VERY USEFUL, BECAUSE YOU
DONT HAVE TO KEEP CONNECTING AND
DISCONNECTING THE FONE (TEST SET)
ITSELF, AND THE CLIP IS DESIGNED TO AID
IN LOCATING THE PAIR AND ASSURING THE
CORRECT POLARITY.

ON THE TERMINAL BOARD, THERE
SHOULD BE ABOUT 20 PAIRS (RED/WHITE)
PER ROW PER SIDE.
HOOK THE CLIP TO ANY TERMINAL PAIR
, AND YOU'RE SET! DIAL OUT IF YOU WANT,
OR JUST LISTEN (IF SOMEONE'S ON THE
LINE). LATER, I'LL SHOW YOU A WAY TO
SET UP A TRUE 'TAP' THAT YOU CAN SET
UP, AND WILL LET THE PERSON DIAL OUT
ON HIS LINE AND RECEIVE CALLS AS
NORMAL, AND YOU CAN LISTEN IN THE
WHOLE TIME. MORE ABOUT THIS LATER...

ON MAJOR PREFIX-AREA BRIDGING
HEADS ('SAI' FOR AREA C.O. FEEDER CABLE
) YOU CAN SEE TEMPORARY 'LOCAL LOOPS',
WHICH ARE TWO CABLE PAIRS (CABLE
PAIR = RING+TIP, A FONE LINE) THAT
ARE DIRECTLY CONNECTED TO EACH OTHER
ON THE TERMINAL BOARD. THESE 'CHEAP
LOOPS' AS THEY ARE CALLED, DO NOT

WORK NEARLY AS WELL AS THE EXISTING
ONES SET UP IN THE SWITCHING HARDWARE
AT THE EXCHANGE OFFICE. (TRY SCANNING
YOUR PREFIXES' 00XX OR 99XX #'S.
THE TONE SIDES WILL ANNOUNCE THEMSELVES
WITH THE 1000 HZ LOOP TONE, AND THE
HANG SIDE WILL GIVE NO RESPONSE. THE
FIRST PERSON SHOULD DIAL THE 'HANG'
SIDE, AND THE OTHER PERSON DIAL THE,
TONE SIDE, AND THE TONE SHOULD STOP
IF YOU HAVE GOT THE RIGHT LOOP).
THE LOOPS ARE USED IN FRAME TERMINATI
ON AND IN SONIC/600 OHM TERM. TESTING
AND LINE/CABLE/FEEDER LOCATION.

IF YOU WANT TO FIND THE NUMBER
OF THE LINE THAT YOU'RE ON, YOU CAN
EITHER TRY TO DECIPHER THE 'BRIDGING
LOG' (OR WHATEVER), WHICH IS ON THE
LEFT DOOR. IF THAT DOESNT WORK, YOU
CAN USE THE FOLLWING:

ANI # (AUTOMATIC NUMBER INDENTICATION)

THIS IS A TELCO TEST NUMBER
THAT REPORTS TO YOU THE NUMBER THAT
YOURE CALLING FROM (IT'S THE SAME,
CHOPPY 'BELL BITCH' VOICE THAT YOU
GET WHEN YOU REACH A DISCONNECTED #)
(PIP OR ONE OF THE 11X SERIES ANNOUNCE
MENT FRAME MACHINES.)

FOR THE 213 NPA - DIAL 1223
213 NPA - (GTE AREAS) DIAL 114
408 NPA - DIAL 760
914 NPA - DIAL 990

THESE ARE EXTREMELY USEFUL WHEN MESSING
WITH ANY KIND OF LINE TERMINALS,
FEEDER BOXES, ETC.

WHEN FINISHED, BE SURE TO CUT
OFF THE CONNECTOR AND TAKE IT WITH YOU
(THEY ARE VERY HANDY), AND CLOSE/LATCH
THE BOX TO AVOID SUSPICION.

****

"CANS" - AERIAL-MOUNTED (TELEPHONE POLE
------ TERMINAL) BRANCH FEEDER CABLE
SPLITTER.

BASICALLY, TWO TYPES:

1> MS3A SERVICE AREA INTERFACE.
(LARGE, RECTANGULAR SILVER BOX AT
THE END OF EACH STREET.)

2> SERIES 600 LOADING COIL, INCLUDES
THE MSX AERIAL DROP SPLITTER.
(BLACK, ROUND OR RECTANGULAR THING
AT EVERY TELEPHONE POLE.)

TYPE 1 - THIS IS THE CASE THAT TAKES THE UNDERGROUND CABLE FROM THE BRIDGER AND RUNS IT TO THE AERIAL BRANCH FEEDER CABLE (THE LOWEST, LARGEST WIRE ON THE TELEPHONE POLE). THE BOX IS ALWAYS ON THE POLE NEAREST THE BRIGING HEAD, WHERE THE LINE COMES UP. LOOK FOR THE 'CALL BEFORE YOU DIG - UNDERGROUND CABLE' STICKERS..

THE CASE BOX IS HINGED, SO IF YOU WANT TO CLIMB THE POLE, YOU CAN OPEN IT WITH NO PROBLEMS. THESE USUALLY HAVE 2 ROWS OF TERMINAL SETS. (TOTAL APPROX. 200-600 PAIRS, DEPENDING ON THE AREA.) THESE ARE ALL THE CABLE PAIRS FOR YOUR STREET.
. (ITS SIMILAR TO A MINIATURE BRIDGING HEAD). USE/ABUSE IT IN THE SAME MANNER AS WE DID BEFORE. (NOTE: ALL THE ACTIVE LINES CARRY FROM 15 TO 48 VDC, AND EVEN 90VAC (WHEN RINGING), SO BE CAREFUL - IT'S NOT GOING TO HURT YOU, BUT IT CAN SURPRISE YOU (AND IF YOU'RE HANGING BY ONE HAND FROM A TEL. POLE, IT >CAN< BE HARMFUL!))

OH, BY THE WAY, IF YOU USE ANI ON EVERY PAIR AND YOU FIND ONE THAT ISNT IN USE ON YOUR STREET, YOU CAN HOOK IT UP FOR YOURSELF (ALMOST). ALSO, YOU HAVE TO BE ABLE TO IMPERSONATE A TELCO TECHNICIAN AND REPORT THE NUMBER AS 'NEW ACTIVE' (GIVING A FAKE NAME AND FAKE REPORT, ETC) I DONT RECOMMEND THIS AND IT PROBABLY WONT (ALMOST POSITIVELY WONT) WORK, BUT THIS IS BASICALLY WHAT TELCO LINEMEN DO).*

* THE USE OF THE 'TEST BOARD' (A 7D# FOR LINEMEN TESTS, OFTEN FOUND NXX-0003 OR NXX-0004) IS BEYOND THE

SCOPE OF THIS ARTICLE, BUT WILL BE
COVERED IN A FUTURE ARTICLE.

TYPE 2 - THIS IS THE SPLITTER BOX FOR
THE AERIAL DROP WIRES FOR THE GROUP OF
HOUSES AROUND THE POLE.
(USUALLY 4 OR 5 HOUSES). USE IT
LIKE I MENTIONED BEFORE. THE TERMINALS
(20 OR SO) WILL BE IN 2 HORIZONTAL
ROWS OF SETS. THE EXTRA WIRES THAT ARE
JUST 'HANGING THERE' ARE PROVISIONS
FOR EXTRA LINES TO RESIDENCES (1 EXTRA
LINE PER HOUSE, THATS WHY THE INSANE
CHARGE FOR LINE #3). IF ITS THE BOX FOR
YOUR HOUSE ALSO, HAVE FUN AND SWAP
LINES WITH YOUR NEIGHBOR! 'PIGGYBACK'
THEM OR USE A CHEESEBOX FOR A LOOP-ARO
UND, ETC.
AGAIN, I DONT RECOMMEND THIS, AND ITS
DIFFICULT TO DO IT CORRECTLY. (ALTHOUGH
USEFUL)

! electronic toll fraud devices !

investigative procedures
--------------- -----------

this section reviews the investiga tive
procedures used by the security
department of ma bell.

most of the discussion will concern
blue box investigations because of the
frequency of the blue box cases
referred to law enforcement officials
for prosecution.

the security department may initially
discover evidence of etf activity. This
may result from an analysis of calling
patterns to particular numbers. Such
analyses may reveal abnormal calling
patterns which possibly are the result
of etf activity
. Moreover, cases of suspected etf are
referred to the security department
from the various operating departments

of bell, from other telephone companies , or from law enforcement officials. In some instances, detection and identification of a calling station originating suspected blue box tones can be provided by use of a special non-monitoring test equipment.

if initial indications are that there is a substantial possibility that a blue box is being used on a particular line, the security department determines certain information about the line. The name of the subscriber to that line is identified, and an inventory is made of the line and station equipment being provided to him. A discreet background investigation (record) is conducted to establish the subscriber's identity. after this preliminary data is gathered , etf detection units are installed on the suspected line to establish "probable cause" for further investigation. If the "probable cause" equipment indicates repeated etf activity on the line, other equipment is then installed to document such activity.

the "probable cause" equipment ascertains the presence of multi-frequency tones on the subscribers end of the line which would not be present in normal usage. The "probable cause" device now being used by some bell central offices register each and every application of 2600hz tones in single-frequency (sf) signalling and/ or 2600hz tone followed by kp tones used in multi-frequency (mf) signalling . As previously stated, such tones should not normally be present on the line.

if "probable cause" is established, other detection, indentification and documentation equipment is installed. the primary equipment now being used is the dialed number recorder (dnr), coupled with an auxillary tape recorder. The dnr is activated when the suspect subscriber's phone goes "off-hook" andb prints on paper tape the following information concerning

the call: the date and time of the call and the digits dialed over the suspects line. Moreover, the dnr records on the paper tape an indicator of the presence of 2600hz tones on the line and the presence of multi-frequency signalling tones on the subscriber's line. The auxiliary tape recorder is activated *only* after the presence of 2600hz tone on the line is detected by the dnr (indicating the use of a blue box)
. Once the tape recorder is activated, it records the tones being emitted by the blue box, other signalling tones, and the ringing cycle on the called end
. It also records a minimum amount of ensuing conversation for the purpose of
(1) establishing that the fraudulent call was consummated
(2) establishing the identity of the fraudulent caller. The timing duration of the tape recorder is pre-set. A time of one-minute (including pulsing, ringing and conversation) is the stand ard setting; however, if the blue box user is suspected of making overseas calls, the timing may be set for 2 minutes because of the greater time required by the blue box user to complete the call. Upon termination of the call, the dnr automatically prints the time of termination and the date.
it should be pointed out that the presence of 2600hz tones *plus* multi-frequncy signalling tones on a subscriber's line positively establishes that a blue box is being used to place a fraudulent call because such tones are not normally originated from a subscribers line.

once the raw data described above is gathered, the security department collects and formulates the data into legally admissable evidence of criminal activity. Such evidence will establish:
(1) that a fraudulent call was placed by means of an etf device,
(2) that conversation ensued,
(3) that the fraudulent call was placed by an identified individual, and(4)
that such call was not billed to the subscriber number from which the blue box call originated. The evidence which is then available consists of documents

and also of expert witness testimony by telephone company personnel concerning the contents of those documents, the operation of the blue box, and the operation of the detection equipment. (note- similar techniques are used in the investigation of other forms of etf.)

-=-

presentation of evidence to prosecutors

the evidence accumulated by the security department is carefully review ed by the legal department for the purpose of determining whether sufficient evidence exists to warrent the presentation of the evidence to law enforcement officials. If the evidence does warrent such action, it is presented under appropriate circumstances to the proper law enforcement officials . In all cases where prosecution is recommended, a professionally investigated and documented summary of the case will be preparted and presented by the security department to the prosecutor's office. Each case recommended for prosecution will be prepared as completely as possible, usually necessitating little or no pre-trial investigation for the prosecutor. The summary of the case will include the following:

(a) a background of the case with details of the defendant's activities and a summary of all pertinent investigative steps and interviews conducted in the course of the investigation.
(b) identification of witnesses.

(c) synopsis of pertinent points to which each witness can testify.
(d) description of all documents and items of evidence and the suggested order of proof showing the chronology of events. The physical evidence presented will normally consist of one or more of the following: magnetic

tapes from the auxilairy tape recorder, paper tapes from the dnr, worksheets and notes prepared in connection with the analysis of each fraudulent call, the suspect's toll billing records covering the period during which the fraudulent activity occured, computer printouts which established probably cause or a statement of the source of the "probable cause", and the telephone company records of equipment being provided to the suspect.

(e) upon request, the law applicable to the case.

other pertinent company records will be furnished under subpoena or demand of lawful authority. If an arrest or search warrent is sought, the security representitives will cooperate fully and furnish affidavits required to support the application for the warrent s, nevertheless, upon request, such representatives will accompany the executing officers to assist in the identification of any suspected etf equipment found. The security representitive will also be available to suggest pertinent areas for interrogation of the persons suspected of engaging in the fraudulent activity.

(i hope that this will help most of you who blue box and who commit other various electronic toll fraud crimes to avoid detection of using a dtf. Also it would seem that they could get almost *no* proof if you went to pay phones instead of at your home.)

How to Get into the AT&T Network by Building Your own Mobile Phone.

This article is presented for entertainment and academic study only. It is a violation of Federal laws to operate an unlicensed transmitter or make fraudulent telephone calls. It is not intended nor expected that anyone actually build the devices described. The article is simply a detailed and factual description of something that could be done.

I wrote a file in collaboration with another telephone experimenter of high repute on IMTS (Improved Mobile Telephone Service) posted elsewhere on this board under the title of "Feature Article". This file was downloaded and posted on another BBS in the Midwest. From there it fell into the hands of the Chief of Security of Southwestern Bell. His words to the Sysop, who had been busted for Blue Boxing were, "A person with a knowledge of electronics could use the information in that file to build his own mobile telephone".

I am going to explain in this article how you can build your own mobile phone. If you haven't figured it out already, you will soon see why the security man was concerned.

This article presupposes that you have a working knowledge of two-way radio. If you don't possess this knowledge, get a copy of "The Radio Amateur's Handbook" (readily available from libraries and book stores) and study up on narrow band FM and 2-Meter transmitters. To get everything you will need in one file, I am reprinting the IMTS article here:

Signaling Used in IMTS
(Improved Mobile Telephone Service)

Each mobile telephone channel consists of two frequencies; one for the land base station and one for the mobile phone. The base station uses two tones for signaling:

Idle	2000 Hz
Seize	1800 Hz

The mobiles use three tones:

Guard	2150 Hz
Connect	1633 Hz
Disconnect	1336 Hz

The land base station marks the idle channel by placing the idle tone on it. All the mobiles search for the channel with the 2000 Hz idle tone and lock on to it.

Each mobile phone is assigned a standard telephone number consisting of area code + 7 digits. When a land customer dials a mobile number, the idle tone (2000 Hz) changes to seize (1800 Hz). The number pulsed to the mobile phone contains 7 digits consisting of the area code and last 4 digits of the number. The digits are made up of 50 ms pulses of 2000 Hz separated by 50 ms of 1800 Hz.

If there is a mismatch between the digits sent and the wired ID in the mobile, the mobile drops off and hunts for the idle channel. If the number matches, the mobile will send back an acknowledgement tone of 750 ms of guard (2150 Hz). The base station waits 3 to 4 seconds for this tone. If not received in that time, the calling party gets a recording. If the tone is received, the mobile phone will ring for up to 45 seconds. Ringing is composed of 1800 Hz and 2000 Hz shifting at 25 ms for two seconds then four seconds of 1800 Hz. When the mobile phone is picked up it sends a connect tone of 1633 Hz for 400 ms to tell the base station it has answered. When the mobile hangs up, it sends disconnect, which is 750 ms of 1336 Hz. When the base receives the disconnect tone, it will drop carrier for about 300 ms and go off. If it is the only available channel, it will return to idle.

Now I will describe what happens when a call is originated by a mobile.

When the mobile goes off hook, it sends 350 ms of guard (2150 Hz) followed by 50 ms of connect (1633 Hz). When the base station hears the connect tone, it removes the idle tone and stays quiet for about 250 ms. It then transmits 250 ms of seize (1800 Hz). The mobile then sends 190 ms of guard and starts transmitting the ID sequence at 20 pulses per second. The ID is the area code and last four digits of the mobile's number. The pulses are marked by 25 ms of connect (1633 Hz) followed by 25 ms of either silence or guard tone (2150 Hz). If the pulse is odd, it is followed by silence. If even, it is followed by guard tone. This is used for parity checking. The interdigit time is 190 ms and will be either silence or guard tone depending on whether the last pulse was odd or even. If the last pulse of the last digit in the ID is even it will be followed by 190 ms of guard tone.

When a number is dialed from a mobile phone, 2150 Hz is sent continuously as soon a the dial goes off normal (when the dial is moved from its resting position). Dial pulses representing breaks are marked by 1633 Hz and are sent at 10 pulses per second. A pulse is 60 ms of 1633 Hz with 40 ms of 2150 Hz between pulses.

The most popular mobile telephone channels are located in the VHF high band. More cities are equipped with these channels than any other band. They are listed below.

Mobile Telephone Frequencies

Channel	Base	Mobile
JL	152.51	157.77
YL	152.54	157.80
JP	152.57	157.83
YP	152.60	157.86
YJ	152.63	157.89
YK	152.66	157.92
JS	152.69	157.95
YS	152.72	157.98
YR	152.75	158.01
JK	152.78	158.04
JR	152.81	158.07

****

This is a list of the components you will need to build your own mobile phone:

1. Cassette Tape Recorder.
2. Radio Scanner (Like those used to receive police calls).
3. Mobile phone dialer (build your own).
4. Low Power Transmitter (Modified 2-Meter transmitter 1 - 5 watts).

How to Build a Mobile Phone Dialer

Build a Wien-Bridge oscillator. These are commonly used in red boxes. If you don't have a red box schematic, look up Wien-Bridge in an electronics textbook. Where you would normally connect a frequency adjustment pot, use two multi-turn pots connected in series. Power for the oscillator will be supplied by a 9 volt battery.

Obtain a rotary dial of the type used on rotary telephones. The dial will have four wires coming out of it; two white, one blue, and one green. The two white wires make a connection when the dial is off normal (moved from its resting position). Connect the two white wires in series with one of the leads from the 9 volt battery. The oscillator will be running only when the dial is moved off normal. It works like this: Dial is moved off normal. Circuit is completed between oscillator and battery. Dial goes back to resting position. Circuit is opened.

The blue and green wires go to a normally closed contact in the dial. This contact opens once for each pulse in a dialed digit. For example it opens three times for the digit "3". Connect these two wires (blue & green) across one of the pots in the oscillator. With the dial in its resting position, adjust the other pot for a frequency of 2150 Hz (Guard tone). Move the dial until the contact opens and adjust the pot with the blue and green wires going to it for a frequency of 1633 Hz (Connect tone).

When the dial is moved off normal, power will be applied to the oscillator, and it will begin running at 2150 Hz. When the dial is released the short across the second pot will be removed each time the contacts open for a dial pulse. During these pulse times the frequency will shift down to 1633 Hz. When the dial gets back to its resting position, power will be removed from the oscillator. This will exactly duplicate the dial pulsing of a mobile telephone.

The Transmitter

Antennae used by mobile phone base stations are located on high towers. This allows line-of-sight transmission to and from the mobiles. If you are within a few miles of a base station very little power is needed to establish contact. 1 to 5 watts should be completely adequate. The less power you use, the less your chances of getting caught. More on this later.

2-Meter transmitters, used in amateur radio, operate in the range of 144 to 148 Mhz. With a change of crystals and a little retuning, you have your transmitter.

How to use Your Home brew Mobile Telephone

With your scanner, locate the base station frequency which currently has the idle tone on it. Switch to the mobile frequency on that same channel and monitor it with the cassette recorder running continuously. What you want is a clean recording of a mobile unit broadcasting its ID sequence. You also want a recording of the disconnect tone when he hangs up. Once you have these, rewind the tape to the start of the sequence. Now you are ready to make a call.

The procedure For Placing a Call

1. Set your scanner to the base station frequency with the idle tone and leave it there. Monitor with earphones to avoid audio feedback through the transmitter.

2. Set the transmitter to the corresponding mobile frequency. Turn it on and leave it on.

3. Play the taped ID sequence.

4. Use your dial pulser to call the desired number. If all has gone well, you will hear your dial pulses in the earphones. You can use this method to call one of the special 800 numbers and whistle off with 2600 Hz; then MF to

anywhere in the world. This technique will reduce your visibility on the bill for the ID you are using.

5. When you are ready to hang up, play the disconnect tone and switch off the transmitter.

A Few Notes About Your Own Security

You should use only as much transmitter power as necessary to maintain a reliable contact. If you do much of this kind of experimenting, the FCC is going to be after you with direction finding equipment. These use directional antennae and a process of triangulation to locate illegal transmitters. If you keep your power down, stay mobile, and avoid establishing a pattern of calling at the same time every day, it will be nearly impossible to track you down.

HOW TO CHANGE YOUR TELEPHONE NUMBER ON THE AT&T NETWORK

CONTACT: (INTERNET) NOFRIENDS@AOL.COM

Alright, this file is for those who do not already know how to block their ANI and change it to someone elses. This enables you to use fraud calling cards and there is no way for you to get caught. In addition you can hack AT&T 800#'s without the risk of getting caught.

This works in nearly 75% of the United States. It works in 35% of GTE areas, 100% of BELL AREAS (Except NEW JERSEY!!!), It only works in like 20% off ALLTEL areas. In other words, if your local exchange carrier subcontracts AT&T for the local operator, this program isn't gonna work unless you have old non-ESS/DMS switching. Unfortunately, this does not work from CANADA.

I'm going to use Pittsburgh, PA and NEW YORK CITY as examples. Figure out your area and it'll be simple.

My understanding is AT&T is unregionalizing their OPERATOR network and soon we can say we are anywhere, but here goes.

==================

If you are calling from (412) PITTSBURGH, PA, you can change your number to anywhere in 412,215,717,814,201,908,609, and 304. Because the Pittsburgh Operator Centers are Mercerville, NJ; Pittsburgh, PA; Charleston, WV; and Somewhere else in NJ.

So, pick the number of your local AT&T Office. That's always what you should use because it pisses them off. They know about this probleam and there is nothing they can do.

I use 412-227-7000

If you are calling for NEW YORK CITY, you can only use NEW YORK area codes (until about 6 months). That means pick something from 212,516,914,718, etc... get the # of AT&T from the phone book. Even if it is a phone center store.

NOW, here goes:

INSTRUCTIONS

Dial 1-800-321-0288. Does it go "BONG AT&T" If so, then you can place 0+ calls and AT&T knows your number. It used ANI to track you. If an operator comes on and says, "CAN I HAVE THE NUMBER YOU ARE CALLING FROM PLEASE?" Then you have an old switch analog switch. Kool.

Now, Dial 0. Ask the operator to dial 1-800-321-0288 for you. If she bitches, explain that you are handicapped and can not dial it yourself. If, by chance, they always bitch, call your local business office and ask that they put a handicapped flag on your account. The operator will quit bitching.

What happens?

In 75% of the country, the AT&T Operator will come on and ask you the number that you are calling from. She'll then get you the number you want even an AT&T 800#. The # you give her will appear on the 800# bill or telephone bill that you are scamming. YOUR NUMBER WILL NOT.

If you receive a recording when the operator puts through the 800-321-0288 number, try again. If it happens twice, guess what, AT&T is your local operator (found alot in GTE and ALLNET areas). There is no way to block it using this method from your area. Find a different way to do it.

HOW LONG WILL THIS LAST?

Well, the FCC ordered AT&T to start 800-321-0288 and leave it open for all callers in the USA. So, therefore it will work in all areas that have an analog tandem (95% of the USA).

Most states have asked the Bell Companies to submit plans to create a fiber network. Most say it will be completed by around 2015. In fact, that's when Bell of PA says it will be done. Note, New Jersey Bell already has a fiber system and there there is no way to block your ANI using the local operator.

Notes: This article is written by Tesla of the Long Island 25. The LI-25 is a closed group, but feels the information should be public. The LI-25 will be releasing very damaging articles about AT&T in the future. I figure we can get away with free calls for the next 10 years on AT&T.

We have known about many flaws in the network, however,

we have kept quiet. Now it's time to talk. AT&T are
rotten bastards and we will prove this. These articles
are in retaliation for "USA vs. Keith Maydak, et al"
Case 93-133 in the US DISTRICT COURT of Western PA.
While Keith Maydak does not condone our activities, we
are simply not please. The outcome will determine AT&T's
balance sheet.

Feel free to pass this article around and add any additional
information at the bottom, but place don't remove this
notation.

AT&T: It's all another part of the I-SCAM!

Getting money from a payphone requires only a few simple things.
1.Intellegence-You have to know when to do this kind of thing. If you do it in
broad daylight, with a bunch of people watching you, you'll have the TELCO on
you so fast you won't know what happened
2. You must select a phone that you can have access to its wires. (Look for a pl
astic shroud running down the wall, or the junction box outside!) On a normal ph
oneline, only two wires are used:Ring & Tip. (Red & Green). The payphone uses th
e red and green
for its telephone operations, but it also uses the yellow & black to control th
e coin mech. relays &   solenoids. Find a section of the wire   where a cut wil
l not be easily seen.   Strip off the insulation of the cord,   exposing the fo
ur wires. Now,
get out
the all purpose wire cutters (Or finger nail clippers if you like) and cut the
black & yellow wires. Now just sit back and let people use the phone!

What Happens? Well, when you put money into a payphone, it stays in the coin
mechanism until 1 of 2 things happen.
1. You connect your call, talk, and Hangup. After you hangup, your money goes
to the collection box. (The only way to get the money then is to rip the box out
!)
2. You call a number that doesn't answer, or get busy signal, or something lik
e that, and then hangup. When you hangup, the money goes from the coin mech. to
the coin return.

That is the key! After the Black & Yellow wires have been cut, the money goes
neither to the coin box or coin return! It just sits there! All you have to do
is come back at like 3:00 in the morning, re-connect the black & Yellow wires,
pick up the han
dset & put it back down.
**********JACKPOT********** All the   money that was put in that phone that da
y comes shooting out the coin return.   (Just like in the movies!) It is the
AWESOMEIST FEELING! I have collected upto $30 a day doing this to phones all
around town!

Dangers: The people that put money in   and don't get connected or get a busy
signal and hang up do NOT get their money back. Usually they will call the
operator who inturn calls the Repair Dept. (That is why it is important to cut
the wire where
it can not be seen. But if you want to do this as a one time thing.........GO F
OR IT! Oh yes, alternate phones every other couplple of days or so. Stay on you
r toes and watch out for white Vans!!!!) If someone sees you taking money out of
the coin retur
n (Getting $15 in change out of a phone is not common!) Just say you hung up the
phone and all this mony started pouring out! (It doesn't hurt to give them a li
ttle of it either!) After a month or two the Phone Co. catches on, so I do not
reccomend using one phone for over two weeks.