###
<*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*>
<*><*><*><*><*>
<*>   Joe Cosmo Presents.....
<*>
<*>
<*>
<*>   Methods of Phreaking and Telco Security
Measures   <*>
<*>
<*>
<*>   June 16, 1988
1:30 am   <*>
<*>
<*>
<*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*><*>
<*><*><*><*><*>

(formatted to 80 Columns)

Dedication: This phile is dedicated to all those great phreakers who taught me all of this, and to all of the newcomers being born to the phreak world. For the legends, it is here as their legacy, and for the newcomers, I hope they will use it as their guide in times of trouble, and may there always be phreakers in the world.

TABLE OF CONTENTS

CHAPTER

I. Introduction: What Telephone Fraud Is

Telephone fraud is illegally using the communication facilities of telephone companies. This is commonly known as "phreaking." The writer's purpose is to explore the methods of phreaking, and the various security measures of telephone companies.

II. Who Does It and Why

The majority of people who phreak are owners of modems (MOdulators DEModulators, devices which allow computers to communicate over telephone lines) and are usually between the ages of twelve and seventeen. When the person reaches age eighteen, he or she usually stops, since after that age, if the person in caught, the penalty can become very serious, such as time in prison, and fines starting at $8000.

Scattered throughout the country are many different computer bulletin board systems, or BBS's. These are computer systems established by private users or large organizations for the exchange of public and private messages and software. Most are not a local call, though. Since the normal user calls about ten different BBS's, with even the lowest long-distance rates, the phone bill each month can range from $100 to $1000. The solution is to phreak. When these people learn how to phreak, they also realize that besides making free long-distance calls from their home, they can also make free calls from payphones. They also find that there are many other facilities that they can used without paying.

III. The Systems That Are Fooled

Their are three types of telephone operating systems in the U.S., Step by Step (SxS), Crossbar (XB), and Electronic Switching

System (ESS). They are
described in detail in the following paragraphs.

Step by Step

Step by Step (SxS) was the first switching system used in America,
adopted in 1918 and until 1978 Bell had over 53% of all exchanges using Step
by Step. A long, and confusing train of switches is used for SxS switching.

Disadvantages

A. The switch train may become jammed, blocking calls.
B. No DTMF (Dual-Tone Multi-Frequency), to be discussed later.
C. Much maintenance and much electricity.
D. No "Touch-Tone" dialing.

Identification

A. No pulsing digits after dialing or "Touch Tone".
B. Much static in the connections.
C. No Speed calling, Call forwarding, and other services.
D. Pay-phone wants money first before dial-tone.

Crossbar

Crossbar has been Bell's primary switcher after 1960. Three types of
Crossbar switchings exist, Number 1 Crossbar (1XB), Number 4 Crossbar (4XB),
and Number 5 Crossbar (5XB). A switching matrix is used for all of the phones
in an area. When someone calls, the route is determined and is connected with
the other phone. The matrix is positioned in horizontal and vertical paths,
organizing the train of switches more effectively, and therefore, stopping
the equipment from jamming. There are no definite distinguishing features of
Crossbar switchings from Step by Step.

Electronic Switching System

ESS is the most advanced system employed, and has gone through many
kinds of revisions. The latest system to date is ESS 11a, which is used in
Washington D.C. for security reasons. ESS is the country's

most advanced
switching system, and has the highest security system of all. With its many
special features, it is truly the phreaker's nightmare.

Identification

A. Dialing 911 for emergencies.
B. Dial-tone first for pay-phones.
C. Calling services, including Call forwarding, Speed dialing, and Call
   waiting.
D. Automatic Number Identification for long-distance calls (ANI), to be
   discussed later.
E. "Touch Tone"

IV. Electronic Toll Fraud

The ETF's are electrical devices used to get free long-distance calls.
The devices are more commonly known as colored boxes, and using them is known
as "boxing." Boxing is one of the oldest way to phreak, and therefore, it is
also the most dangerous, since the telephone companies are very much aware of
their existence. Colored boxes are not used only for phreaking. There are
many types which have other uses (such as the Tron Box, which lowers your
electric bill), so only those used in telephone fraud will be discussed.

How Boxes Work

In the beginning, all long distance calls were connected manually by
operators who passed on the called number verbally to other operators in
series. This is because pulse (rotary) digits are created by causing breaks
in the DC current. Since long distance calls call for routing through
various switching equipment and AC voice amplifiers, pulse dialing cannot be
used to send the destination number to the end local office (CO).

Eventually, the demand for faster and more efficient long distance

service caused Bell to make a multi-billion dollar decision. They had to create a signaling system that could be used on the LD Network. They had two options:

[1] To send all the signaling and supervisory information (eg., ON and OFF HOOK) over separate data links. This type of signaling is referred to as out-of-band signaling.

[2] To send all the signaling information along with the conversation using tones to represent digits. This type of signaling is called in-band signaling.

The second seemed to be the most economical choice, and so, it was incorporated in ESS.

Then, in the 1960's, when the first ESS systems were employed, a toy whistle was put in each box of Captain Crunch Cereal as a premium. A young radio technician in the United States Air Force became fascinated with the whistle when he discovered that by blowing it into the telephone after dialing any long distance number, the trunk line would remain open without toll charges accounting. From then on, any number could be dialed for free. The truth was that the whistle produced a perfect-pitch 2600 Hz tone, the one used to signify a disconnect in ESS switching equipment. To overcome the initial charge for the for the long distance call, he later used toll-free 800 numbers.

Being a skilled technician, Captain Crunch (he began to use the name as an alias) soon went beyond the simple whistle and experimented with other frequencies, creating many of the boxes discussed in the following paragraphs.

The Blue Box

The "Blue Box" was so named because of the color of the first one discovered by the authorities. The design and hardware used in the Blue Box is very sophisticated, and its size varies from a large piece of apparatus to a miniaturized unit that is approximately the size of a "king size" package of cigarettes.

The Blue Box contains 12 or 13 buttons or switches that emit the multi-frequency tones used in the normal operation of the telephone toll (long distance) switching network. In effect, the the Blue Box can let a person become the operator of a phone line. The Blue Box enables its user to originate fraudulent toll calls by circumventing (fooling) toll billing equipment. The Blue Box may be directly connected to a phone line, or it may be acoustically coupled to a telephone handset by placing the Blue Box's speaker next to the transmitter, or the telephone handset.

Operation of a Blue Box

To understand the steps of a fraudulent Blue Box call, it is necessary to understand the basic operation of the Direct Distance Dialing (DDD) telephone network. When a DDD call is originated, the calling number is identified as an integral part of establishing the connection. This may be done either automatically by ANI in ESS, or in some cases, by an operator asking the calling party for his telephone number. This information is entered on a tape in the Centralized Automatic Message Accounting (CAMA) office. This tape also contains the number assigned to the trunk line over which the call is to be made. The information relating to the call contained on the tape includes the called number's identification, time of origination of the call, and if the called number answered the call. The

time of
disconnect is also recorded. The various data entries with
of the call are
correlated to provide billing information for use by the
caller's telephone
company's accounting department.

The typical Blue Box user usually dials a number that
will route the
call into the telephone network without charge. For example,
the user will
very often call a well-known INWATS (toll-free) number. The
Blue Box user,
after gaining this access to the network when somebody picks
up and in
effect, "seizing" control of the line, operates a key on the
Blue Box which
emits a 2600 Hertz (cycles per second, abbreviated as Hz)
tone. This tone
causes the switching equipment to release the connection to
the INWATS
customer's line. The 2600 Hz tone is the signal to the
switching system that
the calling party has hung up. In fact though, the local
trunk on the calling
party's end is still connected to the toll network. The Blue
Box user now
operates the "KP" (Key Pulse) key on the Blue Box to notify
the toll
switching equipment that switching signals are about to be
emitted. The user
then pushes the "number" buttons on the Blue Box
corresponding to the
telephone number being called. After doing so, he/she
operates the "ST"
(Start) key to tell the switching equipment that signaling
is complete. If
the call is completed, only the portion of the original call
prior to the
operation of the 2600 Hz tone is recorded on the CAMA tape.
The tones emitted
by the Blue Box are not recorded on the CAMA tape.
Therefore, because the
original call to the INWATS number is toll-free, no billing
is rendered in
connection with the call.

The above are the steps in a normal operation of a Blue
Box, but they

may vary in any one of the following ways:

A. The Blue Box may include a rotary dial to apply the 2600Hz tone and the switching signals. This type of Blue Box is called a "dial pulser" or "rotary SF" Blue box.

B. A magnetic tape recording may be used to record the Blue Box tones. Such a tape recording could be used in lieu of a Blue Box to fraudulently place calls to the phone numbers recorded on the magnetic tape.

All Blue Boxes, except "dial pulse" or "Rotary SF" Blue Boxes, must have the following four common operating capabilities:

A. It be able to emit the 2600 Hz tone. This tone is used by the toll network to indicate, either by its presence or its absence, an "on hook" (idle) or "off hook" (busy) condition of a trunk line.

B. The Blue Box must have a "KP" tones that unlocks or readies the multi-frequency receiver at the called end to receive the tones corresponding to the called phone number.

C. The Blue Box must be able to emit DTMF, tones used to transmit phone numbers over the toll network. Each digit of a phone number is represented by a combination of two tones. For example, the 2 is 700 Hz and 900 Hz.

D. The Blue Box must have an "ST" key which consists of a combination of two tones that tell the equipment at the called end that all digits have been sent and that the equipment should start connecting the call to the called number.

The following is a chart of the multi-frequency (MF) tones produced by the normal Blue Box.

```
700  :   1   :   2   :   4   :   7   :  11   :    2600 X
900  :   +   :   3   :   5   :   8   :  12   :
1100 :   +   :   +   :   6   :   9   :  KP   :
1300 :   +   :   +   :   +   :  10   :  KP2  :
1500 :   +   :   +   :   +   :   +   :  ST   :
     : 700   : 900   :1100   :1300   :1500   :
```

The "Dial Pulser" or "Rotary SF" Blue Box requires only a dial with a signalling capability to produce a 2600 Hz tone.

Pink Noise

Since telephone companies have such advanced equipment to detect Blue Boxes, to help avoid detection "pink noise" is sometimes added to the 2600 Hz tone.

Since 2600 Hz tones can be simulated in speech, the detection equipment of the switching system must be attentive not to misinterpret speech as a disconnect signal. Thus, a virtually pure 2600 Hz tone is required for disconnect. This is also the reason why the 2600 Hz tone must be sent rapidly; sometimes, it will not work when the person called is speaking. It is feasible, though, to send some "pink noise" along with the 2600 Hz. Most of this energy should be above 3000 Hz. The pink noise will not reach the toll network, where we want our pure 2600 Hz to hit, but it will go through the local CO and thus, the fraud detectors.

The Black Box

The Black Box is the easiest type to build. The box stops a call from being charged to some one only if it is hooked to the line of the person being called.

In the normal telephone cable, there are four wires: a red, a green, a black, and a yellow. The red & green wires are often referred to as tip (T) and ring (R).

When a telephone is on-hook (hung up) there is approximately 48 volts of DC current (VDC) flowing through the tip and ring. When the handset of a phone is lifted, switches close, causing a loop to be connected (which is known as the "local loop,") between the telephone and the CO. Once this happens DC current is able to flow through the telephone with less resistance. This causes a relay to energize and signal to other CO equipment that service is being requested. Eventually, a dial tone is emitted. This also causes the 48 VDC to drop down into the vicinity of 13 volts. The resistance of the loop also drops below the 2500 ohm level. Considering that this voltage and resistance drop is how the CO detects that a telephone was taken off hook, how a Black Box works is by allowing the voltage to drop enough to allow talking, but not enough to signal to the CO equipment to start billing. To do this, a 10,000 Ohm, .5 Watt resistor is incorporated in the local loop on the called party's line.

The Red Box

A Red Box is a device that simulates the sound of a coin being accepted by a payphone. When a coin is put in the slot of a payphone, the first obstacle is the magnetic trap. This will stop any light-weight magnetic slugs. If it passes this, the coin is then classed as a nickel, dime, or quarter. Each coin is then checked for appropriate size and weight. If these tests are passed, it will then travel through a nickel, dime, or quarter magnet as proper. These magnets start an eddy current effect which causes coins of the appropriate characteristics to slow down so they will follow the correct trajectory.

If all goes well, the coin will follow the correct path, striking the

appropriate totalizer arm, causing a ratchet wheel to rotate once for every 5-cent increment (eg, a quarter will cause it to rotate 5 times). The totalizer then causes the coin signal oscillator to readout a dual-frequency signal indicating the value deposited to the Automated Coin Toll Service computer (ACTS) or the Traffic Service Position System (TSPS) operator. These are the tones emitted by the Red Box.

For a quarter, five beep tones are outpulsed for 66 milliseconds (ms). A dime causes two beep tones for 33 ms, while a nickel causes one beep tone at also 33 ms. A beep consists of two frequencies, 2200 Hz and 1700 Hz. As with a Blue Box, Red Box tones can be recorded on a magnetic tape.

Since any call from a payphone is originated with a "ground test," in which the TSPS operator or the ACTS computer checks for the presence of the first coin inserted into the phone, by verifying use of the magnetic, weight, and size traps, when using a Red Box, it is necessary to put in at least one coin.

The Cheese Box

A Cheese Box lets a normal telephone emulate a payphone. By emulating a payphone, using a blue box now becomes safe, because if the CO equipment recognizes the call as one from a payphone, it does not record it on a CAMA tape. Since a normal telephone does not have a slot to enter coins, a Red Box is needed to generate the sound of a coin dropping.

V. Divertors

A divertor is a special service that allows businesses to "divert" calls if no one answers after a certain number of rings. For example, a person calls a company, and nobody answers. After about three rings, a few clicks are heard, then a few fainter rings are heard. The building

receiving the call has changed from the company to another building, usually somebody's house. What has happened is that the call has been re-routed from building A to building B. In effect, the number called is not really changed, but instead, building A has answered the call, called building B, and connected the two lines together. If the person in building B disconnects, the caller is still connected to building A. With the way the divertor equipment works in the telephone company, the phone line of building A will then emit a dial tone and the caller has total control of the line, and can originate another call, charging it to building A.

VI. Private Branch Exchanges

A Private Branch Exchange (PBX) is a system of out-WATS (Wide Area Telephone Service) lines and in-WATS lines. An out-WATS line allows a business to make as long-distance calls each month for a flat rate. An in-WATS line is a toll-free number (800 number) that is also leased to businesses for flat rates. PBX's save corporations much money when their salesmen, distributors, and franchisees must make many calls from different parts of the country. It works much like specialized common carriers (to be discussed later).

First, the employee calls the company on the in-WATS line. The switching equipment picks up the phone, and send a tone to the employee indicating for him to enter the access code of the PBX. If the access code is correct, then the line is connected to the out-WATS line, and the employee can make a call.

To use PBX's, phreakers must find the access code of the PBX. This can be done very easily, since the code is usually only a few digits. One way is

to dial different combinations manually on the telephone keypad. The other way is of the phreaker is the owner of a modem. A simple program can be easily written to continuously dial digit combinations randomly or sequentially.

VII. Specialized Common Carriers

Ever since the break up of AT&T's monopoly on long-distance service, there have been many other corporations that compete with AT&T in the long-distance market, including Sprint, MCI, All-net, ITT, and Metrophone. These all boast opportunities for large savings on long-distance calls. These companies are called specialized common carriers (SCC's).

SCC's cost less because they do not use the AT&T's cable-based systems, but instead use microwave links. Some have also added fiber-optic lines to their networks.

Another way they can save consumers money is by using AT&T's lines. Instead of connecting calls by the shortest route, the carrier will use a different route, so the call goes through places where the long-distance traffic is heavy, and the rate is lower. The companies that do this are known as "resellers."

Most SCC's work nearly the same as PBX's. The 800 number is called, a tone is heard, the private identification number (PIN) is entered, and then the call can be made. The length of the PIN number can range from four digit to fourteen digits.

Besides 800 toll free numbers, in some areas, a 950 can be used. A 950 works exactly the same as an 800 number, the only difference is that the consumer must enter only seven digits before dialing his PIN number instead of ten with a toll-free number. 950's are free of charge and can be used both

at home and at pay phones.

The PIN numbers can be found the same way as PBX access codes. Since the number of digits in a PIN is so great, using a computer is much more common practice than manual dialing.

The following pages are lists of SCC's and their dialups, formats, and special points. Note that some have many different dialups.

```
============================================================
=================
[                          SCC Extenders List
]
[                     0-9 - Number of digits in code
]
[                     [ ] - Dial that exact number
]
[                     #   - Area code + Prefix + Suffix
]
[                     :   - Dial tone
]
[                     +   - ontinue dialing
]
============================================================
=================
|   Extender   |  Dialing Format  |        Company        |
Comments    |
------------------------------------------------------------
-----------------
| 800-223-0548 | 8+[1]+#          | TDX                   |
|
| 800-241-1129 | 8+[1]+#          | TDX                   |
|
| 800-248-6248 | 6+[1]+#          | SumNet Systems        |
(800)824-3000   |
| 800-288-8845 | 7:[1]+#          | TMC Watts             |
(800)999-3339   |
| 800-325-0192 | [1]+#+6          | MCI                   |
950-1986       |
| 800-325-1337 | 7:[1]+#          | TMC Watts             |
|
| 800-325-7222 | 6+[1]+#          | Max                   |
(800)982-4422   |
| 800-325-7970 | 6+[1]+#          | Max                   |
(800)982-4422   |
```

| 800-327-4532 | 8+# | All-TelCo |
|
| 800-327-9488 | #:13 | ITT |
950-0488 |
| 800-334-0193 | [9]+# | Piedmont |
|
| 800-345-0008 | [0]+#:14 | US Sprint FON Cards
|950-1033 also 9+#|
| 800-368-4222 | 8+# | Congress Watts Lines |
|
| 800-437-7010 | 13 | GCI |
|
| 800-448-8989 | 14+[1]+# | Call US |
|
| 800-521-8400 | 8:# | TravelNet |
950-1088 (voice)|
| 800-541-2255 | 10 | MicroTel |
|
| 800-547-1784 | 13 | AmericaNet |
|
| 800-621-5640 | 6+[1]+# | ExpressTel |
|
| 800-637-4663 | 5+[1]+# | TeleSave |
|
| 800-821-6511 | 5+[1]+# | American Pioneer |
(800)852-4154 |
| 800-821-6629 | 6+[1]+# | Max |
(800)982-4422 |
| 800-821-7961 | 6+[1]+# | Max |
(800)982-4422 |
| 800-826-7397 | 6:[1]+# | Call U.S. |
|
| 800-858-4009 | 6+[1]+# | NTS |
Voice |
| 800-862-2345 | 7:[1]+# | TMC |
|
| 800-877-8000 | [0]+#:14 | US Sprint Calling
Card|950-1033 also 9+#|
| 800-882-2255 | 6:[1]+# | AmeriCall |
False Carrier |
| 800-950-1022 | [0]+#:14 | MCI Calling Card |
|
| 800-992-1444 | 9+# | AllNet |
950-1444 |

VIII. PC Pursuit

Many modem users know Telenet as a packet-switching network through which they can connect to different telecommunication services throughout the country for an hourly rate of $2. With PC Pursuit, Telenet uses the same method as SCC's, but instead of using microwave links, the call is routed through computers. Since it is routed through computers, the service can be used by only owners of modems. Instead of paying the hourly rate, the consumer needs only to pay a flat monthly rate of $25.

Using PC Pursuit is a little more difficult than using SCC's, because now instead of combinations of only ten different characters (0-9), the whole alphabet can be used in the access code. The following is a chart showing the steps to originate a typical PC Pursuit call.

How to Originate a PC Pursuit Call

First, the users dials the local Telenet Access Center, which can be found by dialing Telenet customer service at 1-800-336-0437.

Then:

Note: (cr) signifies the carriage return on a computer keyboard.

Network Shows	User Types	Explanation
	(cr) (cr)	
TELENET		Telenet network called and
XXX XXX		your network address.
TERMINAL=	"D1" (cr)	Enter "D1" or press (cr)

@	For 300 bps:	CONNECT
	"C(sp)DIALXXX/3,XXXX(cr)"	a PC Pursuit city type a PC
		Pursuit access code and
	For 1200 bps:	your user ID.
	"C(sp)DIALXXX/12,XXXX(cr)"	
PASSWORD=	"XXXXXX" (cr)	Type the password
DIALXXX/X	"ATZ" (cr)	You are now connected to the
CONNECTED		PCP city. Type ATZ (upper).
OK	"ATDTXXXXXXX" (cr)	Dials a number in PCP city
CONNECT		Your are now connected to
		your destination computer.

If the number dialed is busy, the user will see BUSY. To call another number in the same city, the user types "ATZ." The network will answer OK. The user then types "ATDTXXXXXXX" (cr) to dial the next number.

To connect to a different PC Pursuit City, when the user sees BUSY, he types "@" (cr). When a @ appears, "D" (cr) is entered. This disconnects the user from the previous city. The user then follows the above procedures to dial another city.

IX. Cellular Phone Fraud

Cellular phones have evolved considerably from previous

systems.
Signaling between mobile and base stations uses high-speed digital techniques
and involves many different types of digital messages. The cellular phone
contains its own Mobile Identification Number (MIN), which is programmed by
the seller or service shop and can be changed when, for example, the phone is
sold to a new user. In addition, the U.S. cellular standard incorporates a
second number, the Electronic Serial Number (ESN), which is intended to
uniquely and permanently identify the mobile unit.

     According to the Electronic Industries Association (EIA) Interim
Standard IS-3-B, Cellular System Mobile Station Land Station Compatibility
Specification, the serial number is a 32-bit binary number that uniquely
identifies a mobile station to any cellular system. It must be factory-set
and not readily alterable in the field. The circuitry that provides the
serial number must be isolated from fraudulent contact and tampering.
Attempts to change the serial number circuitry should render the mobile
station inoperative.

     The ESN was intended to solve two problems the industry observed with
its older systems. First, the number of subscribers that older systems could
support fell far short of the demand in some areas, leading groups of users
to share a single mobile number (fraudulently) by setting several phones to
send the same identification. Carriers lost individual user accountability
and their means of predicting and controlling traffic on their systems.

     Second, systems had no way of automatically detecting use of stolen
equipment because thieves could easily change the transmitted identification.

    In theory, the required properties of the ESN allow cellular systems to
check to ensure that only the correctly registered unit uses

a particular MIN, and the ESNs of stolen units can be permanently denied service ("hot-listed"). This measure is an improvement over the older systems, but vulnerabilities remain.

ESN Tampering

Although the concept of the unalterable ESN is laudable in theory, weaknesses are apparent in practice. Many cellular phones are not constructed so that attempts to change the serial number circuitry renders the mobile station inoperative. Contrary to this statement, swapping of one ESN chip for another in a unit that has been found to functione flawlessly after the switch was made.

Obtaining ESN's

Since most manufacturers are using industry standard Read-Only Memory (ROM) chips for their ESNs, the chips are easily bought and programmed or copied. In programming the ESN with a valid code is another matter. Remembering that to obtain service from a system, a cellular unit must transmit a valid MIN (telephone number) and (usually) the corresponding serial number stored in the cellular switch's database. With the right equipment, the ESN/MIN pair can be read right off the air because the mobile transmits it each time it originates a call. Service shops can capture this information using test gear that automatically receives and decodes the reverse, or mobile-to-base, channels.

Another way to obtain the numbers is from service shops. Service shops keep ESN/MIN records on file for units they have sold or serviced, and the carriers also have these data on all of their subscribers. Unscrupulous employees could compromise the security of their customers' telephones by

obtaining these records.

In many ways, trade in illegally obtained ESN/MIN pairs could, in the future, resemble what currently transpires in the long distance telephone business with AT&T credit card numbers and alternate long-distance carrier (such as MCI, Sprint and Alltel) account codes. Code numbers are swapped among friends, published on computer bulletin boards and trafficked by career criminal enterprises.

X. CN/A's

CN/A's, which stands for Customer Names and Addresses, are bureaus that exist so that authorized Bell employees can find out the name and address of any customer in the Bell System. All phone numbers are maintained on file including unlisted numbers.

To find the owner of any number, the person first must call the local CN/A during business hours. Then he must pretend to be from a registered business, and ask for the owner of the number. In some states, though, the operator will ask for an ID number. In these cases, one must be guessed at.

There is also a type of reverse CN/A bureau, which is usually called a NON PUB DA or TOLL LIB. With these numbers, somebody can find unpublished numbers if the caller gives the operator the name and locality. These are considerably harder to use, since the operator will then request the caller's name, supervisors name, etc.

The following is a list of current CN/A's.

1988 CN/A List (subject to change)

Area: CN/A Area: CN/A Area: CN/A

201: Classified 202: 304-343-7016 203: 203-789-6815

204: 204-949-0900 206: 206-345-4082 207: 617-787-5300

208: 303-293-8777 209: 415-781-5271 212: 518-471-8111

213: 415-781-5271 214: 214-464-7400 215: 412-633-5600

216: 614-464-0519 217: 217-789-8290 218: 402-221-7199

219: 317-265-4834 301: 304-343-1401 302: 412-633-5600

303: 303-293-8777 304: 304-344-8041 305: 912-752-2000

307: 303-293-8777 308: 402-221-7199 312: 312-796-9600

313: 313-424-0900 314: 816-275-8460 316: 913-276-6708

317: 317-265-4834 318: 504-245-5330 319: 402-221-7199

401: 617-787-5300 402: 402-221-7199 404: 912-752-2000

405: 405-236-6121 406: 303-293-8777 412: 412-633-5600

413: 617-787-5300 414: 608-252-6932 415: 415-781-5271

416: 416-443-0542 417: 816-275-8460 418: 614-464-0123

419: 614-464-0519 501: 405-236-6121 502: 502-583-2861

503: 206-345-4082 504: 504-245-5330 505: 303-293-8777

509: 206-345-4082 512: 512-828-2501 513: 614-464-0519

514: 514-394-7440 515: 402-221-7199 517: 313-424-0900

518: 518-471-8111 519: 416-443-0542 601: 601-961-8139

602: 303-293-8777 603: 617-787-5300 605: 402-221-7199

606: 502-583-2861 607: 518-471-8111 608: 608-252-6932

609: Classified 612: 402-221-7199 613: 416-443-0542

614: 614-464-0519 615: 615-373-5791 616: 313-424-0900

617: 617-787-5300 619: 415-781-5271 701:

402-221-7199
 702: 415-543-2861 703: 304-344-7935 704:
912-752-2000
 705: 416-443-0542 707: 415-781-5271 712:
402-221-7199
 713: 713-961-2397 715: 608-252-6932 716:
518-471-8111
 717: 412-633-5600 718: 518-471-8111 801:
303-293-8777
 802: 617-787-5300 804: 304-344-7935 805:
415-781-5271
 806: 512-828-2501 809: 404-751-8871 812:
317-265-4834
 813: 813-228-7871 814: 412-633-5600 815:
217-789-8290
 816: 816-275-8460 817: 214-464-7400 901:
615-373-5791
 904: 912-752-2000 906: 313-424-0900 912:
912-752-2000
                    914: 518-471-8111 916:
415-781-5271
                    918: 405-236-6121 912:
912-752-2000

XI. Loops

The loop is an alternative communication medium that has many potential uses. Loops are phone lines that are connected when they are called simultaneously. One use is when somebody wants another person to call them back but is reluctant to give out their home phone number (eg., if they were on a party line).

Loops are found in pairs that are usually close to each other (eg., 718-492-9996 and 718-492-9997). On a loop, one line is the high end, and the other is the low end. The high end is always silent. The tone disappears on the low end when somebody calls the high end.

It is truly only safe to use a loop during non-business hours. During business, loops are used to test equipment by various

telephone companies and
local CO's.

XII. Alliance Teleconferencing

Alliance Teleconferencing is an independent company which allows the general public to access and use its conferencing equipment.

Billing an Alliance Conference

Alliance Teleconferencing is accessed by dialing 0-700-456-1000 in most states. In some states, the first and last digits of the suffix vary. There are four main ways to use Alliance illegally. The first is through a PBX. Some allow use of the 700 exchange, but many do not.

The second way is with a Blue Box. After seizing the line, KP-0-700-456-1000-ST is dialed. The equipment now thinks that Alliance has been dialed from a switchboard and bills the conference to it.

The third way is to a loop. After being connected to Alliance, the caller contacts the operator by pressing 0. The caller then can ask for the conference to billed to another number, giving the operator the number of the high-end of a loop. The operator will then call the loop. A friend of the phreaker must be prepared to answer the call by calling the low-end. When the friend answers and accepts the billing, the conference will be billed to the loop.

The fourth way is from a divertor. Since the divertor is a normal, home-type line, the phreaker should not have any problems starting a conference.

Starting a Conference

When Alliance answers, a two-tone combination is emitted. The caller then types a two digit combination to tell the equipment how many people will

be in the conference, including the originator. Then either # is pressed to
continue or * is pressed to cancel the conference. To dial a each conferee,
the phreaker simply answers each prompt with the phone number of the
corresponding person.

To join the conference, the originator enters #, and to return to
control mode, he enters # again. To transfer control of the conference,
#+6+1+ the phone number of the person you wish to transfer the control to. To
end the conference, the phreaker presses the * button.

XIII. Telephone System Security Measures

To stop telephone fraud, there are many measures which telephone
companies can apply to identify and convict the phone phreaker.

ESS Detection Devices

Telephone companies have had twenty years to work on detection devices;
therefore, they are well refined. Basically, the detection devices will look
for the presence of 2600 Hz where it does not belong, which is in the local
CO. It then records the calling number and all activity after the 2600 Hz.

Automatic Number Identification and the Centralized Automatic Message Accounting Tapes

Automatic Number Identification (ANI) is an implement in ESS that can
instantly identify the calling party. For every call that is made,
information including the numbers of the calling and receiving parties, the
time of origination of the call, if the called party answered the call, and
the time when the caller has hung-up is recorded on a tape in the Centralized
Automatic Message Accounting (CAMA) office. This includes wrong numbers,
toll-free numbers, and local calls. This tape is then

processed for billing
purposes.

Normally, all free calls are ignored, but the billing equipment has been
programmed to recognize many different types of unusual activity. One checks
if a certain 800 number is called excessively. If the number is an SCC, the
equipment can instantly check if the caller is a subscriber of the SCC. If it
is not, it will alert the company of the illegal activity. Another is if
there is a call where the calling party has stayed off-hook for a large
amount of time, but the called party never answers. The equipment recognizes
this as possible use of a Black Box.

Dialed Number Recorders

Placing a Dialed Number Recorders (DNR) on a telephone line is standard
procedure when telephone fraud is suspected. The most common DNR's can do the
following: print all touch tone digits sent (in suspected illegal use of an
SCC), print out all MF and record the presence of 2600hz on the line (in
suspected use of a Blue Box), and activate a tape recorder for a specific
amount of time.

Trap Codes

Trap codes are decoy PIN numbers. If a telephone company find that a
certain PIN number is being used illegally, it will call the real owner and
notify him of the change in his account number. The company will then contact
the FBI to bring their telephone "lock in" trace equipment.

A lock in trace is a device used by the FBI to lock into the phone
user's location. Since all phone connections are held open by a certain
voltage of electricity,
the lock in trace works by patching into the line and generate the same
voltage into the lines. If the caller tries to hang up, voltage is retained.

The phone will continue to ring as if someone was calling even after the call is disconnected. The trunk then remains open and the call can be traced. The FBI sets its equipment so that the next time the PIN number is illegally used, the call goes through, but while the communication is proceeding, the FBI traces the call.

Stopping an FBI Trace.

Stopping a trace is quite simple. If the voltage in the line could be lowered, the trace could not function, since lowering the voltage would also probably short out the FBI voltage generator. Therefore, any appliance which uses many volt can be connected to the red and green wires in a wall jack, and the trace should be removed.

Common Channel Inter-office Signaling

Besides detection devices, Bell has begun to gradually redesign the network using out-of-band signaling. This is known as Common Channel Inter-office Signaling (CCIS). Since this signaling method sends all the signaling information over separate data lines, and does not use any form of DTMF, all colored boxes do not work under it. Of course, until this multi-million dollar project is totally complete, boxing will still be possible. It will become progressively harder to find places to "box" off of, though.

XIV. Laws Governing the Rights of Phreakers

Since phreaking is one-hundred percent illegal, once discovered, there are not many laws protecting the phreaker. There are, however some laws governing steps government agents may take to convict him.

The first law is the Section 605 of Title 47 of the United States Code. This section forbids interception of communications, except

by persons
outlined in Chapter 119, Title 18, which is a portion of the
Omnibus Crime
Control and Safe Streets Act of 1968.

In this chapter, Section 2511 (2) (a) (i) says "It
shall not be unlawful
under this chapter for an operator of a switchboard, or an
officer, employee,
or agent of any communications carrier, whose facilities are
used in the
transmission of a wire communication, to intercept,
disclose, or use that
communication in the normal course of his employment, while
engaged in any
activity which is a necessary incident to the rendition of
his service of the
protection of the rights or property of the carrier of such
communication."
This means that agents of telephone companies are allowed
not only allowed to
tap lines without a warrant, but also allowed to disclose
the recording of a
communication.

In the case United States vs. Sugden, the following
ruling was made:
"For an unreasonable search and seizure to result from the
interception of
the defendant's communication, he must have exhibited a
reasonable
expectation of privacy. Where, as here, one uses a
communication facility
illegally, no such expectation is required." This simply
means that when you
make an illegal call, you have waved your right to privacy.

.S