Originally Displayed on P-80 Systems

ELECTRONIC TOLL FRAUD DEVICES

BLUE BOXING

The following information applies primarily to the AT&T network. It is the largest long distance carrier and has been around the longest therefor, more is known about its technical operation. The other carriers have their own special weaknesses and are more easily breached using methods described in another chapter.

What is a Blue Box?

The blue box is so named because that happened to be the color of the first one found. A basic blue box contains 13 buttons or switches for the digits 0-9 plus two control signals labeled "KP" and "ST". One of the buttons is used to produce the 2600 Hz "disconnect" signal. Blue boxes are used to circumvent telephone company billing equipment and make free calls to anywhere in the world. The box may be conncted directly to the phone line or acousticaly coupled to the mouth piece of the handset. The signaling tones produced by the box may also be recorded on a cassett tape for later playback. In spite of continuing efforts to protect the system from fraudulent use, there has been a new wave of blue boxing in recent years due to the advent of the personal computer and new knowledge about "holes" in the integrity of the system. A phone preak can buy a personal computer in a department store for less than $200.00. Armed with this hardware and the right knowledge, he can make long distance calls including overseas calls, set up interstate conferences with his friends that go on for hours, call special operators who normally can be reached only by other operators, and other "tricks"; all without charge. With the addition of a cheap cassett recorder, he can become highly mobile and illusive.

Highly advanced and knowledgable phone prheaks are constantly probing the system for flaws in its security. Their ability to call internal operators gives them the power to pose as telephone company personel for the purpose of gaining priviledged information about the system. It would be hard to estimate how many calls from "Telephone Repair Service" or "Security" were actually placed by phone phreaks doing experiments of their own or fishing for information.

How It Works

The most common form of signaling between toll offices uses a code derived from six tones. This is refered to as multifrequency signaling or MF signaling. The tones are played together two at a time to represent the digits 0 - 9. In addition there are two special signals designated KP and ST. These are also sent as dual tones. KP stands for key pulse. It is a gate opening signal which tells the system that digits are to follow. ST means "start transit". It tells the system that all digits have been sent. It is an end of transmission signal and is a command to the system to start processing the information. The principle is basicaly the same as that used for tone signaling with a push button telephone except that the frequecies of the tones are different.

Table (X) shows the combinations of frequencies used in North America and on CCITT Signaling System No. 5:

Signal	Frequency pair
KP1 (start-of-digit transmission for a national call)	1100+1700
KP2 (start-of-digit transmission for an international call from an intermediate (transist) exchange)	1300+1700
Digits: 1	700+900
2	700+1100
3	900+1100
4	700+1300
5	900+1300
6	1100+1300
7	700+1500
8	900+1500
9	1100+1500
0	1300+1500
ST (End of digit transmission)	1500+1700

The MF signals are sent over the normal voice channels. They may be sent by a switchboard operator or by automatic equipment. On some systems the operator's signaling is audible and sometimes the automatic signaling can be heard due to cross talk between lines.

A 2600 Hz tone is transmitted continuously on all voice channels between toll offices when the channel is free. This frequency also acts as a disconnect signal, indicating that the voice channel should return to its unused status.

When a subscriber dials a number it reaches his local central office and possibly toll office by dc pulsing or push button tone signaling. The toll office selects a free voice channel in an appropriate trunk and stops the 2600 Hz tone. The office at the end of that trunk detects the break in the 2600 Hz signal and is alerted to receive a toll telephone number. The number is sent in the MF code listed in table (X). One toll office passes the number to another until the called central office is reached. The central office then rings the called telephone.

When either party hangs up, the call is disconnected and the toll offices start transmitting the 2600 Hz tone again to indicate that the channel is idle.

If a short burst of 2600 Hz is transmitted from a subscriber's telephone, the toll office receives this as a signal that the subscriber has hung up. It then places 2600 Hz on the channel to the next toll office. Phone phreaks call this "whistling off" or "beeping off" a trunk. The subscriber is still connected to a long distance switching office. This is the first step to bypassing the telephone company's billing computer and making free calls to anywhere in the world.

A blue box call is started by dialing a long distance call in the normal way

to a toll free "800" number. Directory assistance numbers can also be used or a call can be placed to a nearby destination which is cheap to call. This is the call which will appear on the CAMA tape. Once dialing is completed, and the called number starts to ring, you feed 2600 Hz into your phone for one second. Experienced phone phreaks familiar with the timing whistle off a second or two before the called number actually rings. The 2600 Hz tone is acousticaly coupled to the phone by simply placing the blue box against the mouth piece and pressing the appropriet button. The local CO is not listening for 2600 Hz to indicate a disconnect. It monitors the current flow in the line and knows the subscriber hung up when the current flow drops below a certain minimum. The 2600 Hz tone is passed on to the toll switching office as if it were a voice signal. The toll office is not listening for 2600 Hz from a CO and so passes it on to the next toll office. At this point the tone is heard as signal that the caller has hung up. The call is cancelled leaving the caller still connected to a toll line between switching offices. After sending 2600 Hz for approximately one second you remove it. The removal of the tone tells the distant switching office that the line is no longer idle. It connects an incoming sender and waits for instructions in the form of MF signaling. At this point you have about ten seconds to start dialing the desired number on the blue box. The number is dialed in a manner simmiler to using a push button telephone. It is in this format: KP+(area code)+(7 digit phone number)+ST.

When the called number answers, a signal is sent back causing the CAMA tape to be punched with the time the connection was made. At the end of the call, the CAMA tape is punched with the number called from, the time and the number you originally dialed. This is the information that will be used to compute your bill. The call will be free if an 800 numer was used. The number actually reached with the blue box is not recorded. Modern systems frequently use magnetic tape instead of punched paper tape to record the billing information but it works the same.

Getting Into the System

Many CO's are now using CCIS (Common Channel Interoffice Signaling). With this system control signaling is done over different lines than those used for voice transmission. If a toll free call is placed from an area using CCIS to another CCIS area, transmitting 2600 Hz will not cause a disconnect. In 1984, just when it appeared that blue boxing was dead except when done from a few areas of the country, advanced "researchers" discovered holes in the system that opened it up again all over the country including nearly every street corner pay phone. New "holes" are constantly being found and usually are soon pluged after it is discovered they are being used to make illegal calls. The main method in use at this time is to call an 800 number that rings into a non CCIS area. Knowledgable phone phreaks predict that all of these "holes" will not be plugged until sometime after the year 2000. By then new and better ways will probably have been developed to beat the system. The trick to using this method is to find an 800 number that rings into one of the few remaining areas that still use the older switching equipment. This is not difficult when you know how. When 2600 Hz is transmitted, it travels over the voice channel to the toll office at the distant end where it is recieved as a disconnect. Usually a "chirp" or "kachink" is heard and you're in!

A few pay phones, especially those located in rural areas, will disconnect

locally if 2600 Hz is played into them. The effect is the same as hanging up the receiver, then picking up again after a few seconds. This is useless for blue boxing and would seem to be an obstical. Actually, it was a delishious challenge to the "researchers" and soon fell as a barrier to boxing under the probing of a few tone combinations. The local disconnect occurs because the local CO is listening for 2600 Hz. The device that does the listening is called a SF (single frequency) unit. These units are designed to disconnect only when 2600 Hz is received without the presence of any other voice band frequencies. This is to prevent accidental disconnects on voice components. To get by this unit, 2600 Hz is played in combination with a second tone in the range of 3400 to 3600 Hz. This is a "guard" tone. When the SF unit hears the higher tone along with the 2600 Hz signal, it does not disconnect. The CO passes the two tones along the voice channel toward the switching office at the distant end. As the tones pass through the long distance network, the higher tone becomes atenuated to a subaudible level. Only the 2600 Hz tone reaches the distant toll office where it produces the desired disconnect. Once again technology triumps in determined hands. The following is a list of 800 prefixes in order by state. The number in parentheses indicates the area code served by that prefix. An asterisk (*) to the left of the prefix indicates that one or more 800 numbers have been found in that prefix which can be whistled off using 2600 Hz. An asterisk to the right indicates that a toll switching office has been located in the area code served by that prefix which will accept MF. There is a lot of research yet to be done on this list. In its present form, it is a road map of great value to the advanced blue boxer.

This system is gradually being replaced by the expanded 800 service. Prefixes in the expanded 800 service have no relationship to area codes, but thousands of numbers are still in place under the old system. Some of the prefixes listed below are easy to hack for blowable numbers. (A "blowable" number is one which will disconnect on 2600 Hz). Look for the ones with asterisks before and after them like this: *XXX*.

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 Col.	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)

How to Make Overseas Calls With a Blue Box

Overseas dialing is done in two stages of outpulsing. The first stage routes to an overseas sender and uses 011, which is the international access code for International Direct Distance Dialing (IDDD) plus the paired country code. If the country code is two digits, the paired country code can be derived by adding a "0" to the left of the country code. Example: The country code for England is 44. The paired country code would be 044. First stage outpulsing for England would then be: KP-011044-ST. If the country code contains three digits, the paired country code cannot be derived in this way and must be looked up. Example: The country code for Guam is 671. The paired country code is 067. First stage outpulsing for Guam would be KP-011067-ST. Second example: The country code for Cyprus is 357. The paired country code is 087. It is a rule that a paired country code must never be the same as any country code.

About five seconds after the STart pulse, an international dial tone will be heard. This will time out to a reorder in about ten seconds.

When the dial tone is heard, the system is ready to accept the second stage of pulsing in the format: KP-country code-city code-digits-ST. At this stage it is the country code not the paired country code which is used.

Use the paired country codes when calling inward operators.

Some toll offices are screened against 011 coming in on a long distance trunk. In that case precede the 011 with the area code which would apply for that toll office. Example: for a toll office in Gainsville, FL use KP-904+011+paired CC-ST.

Another way to reach the overseas senders is to call them directly with KP-sender number-ST. If this doesn't work add the area code of the sender. Example: KP-904185-ST.

This is a list of international centers with their area codes.:

A/C	Sender	Location
914	182	White Plains, NY
212	183	New York, NY
412	184	Pittsburg, PA
904	185	Jacksonville, FL
415	186	Sacramento, CA
303	187	Denver, CO
212	188	New York (same sender as 183)

The routing for a particular country can be found by dialing normally (pulse or touch-tone) 011+CC+000+enough digits to add up to a total of seven including the country code. Example: 011+44+00011. You will get a recording. At the end of the

recording, the area code of the international center will be given. The sender used to call a particular country can vary depending on the area of the country from which the call is originated. An international call can sometimes be completed through the wrong sender, but this causes a print out that will later be investigated to find out which CO it came from. To find the correct routing when pulsing through any particular toll office use KP+paired CC+000+ST. For example, KP-011044000-ST would give the same result as dialing normally 011-44-00011 if you were dialing it in the area where the toll office is located.

The first digit of a country code is the world region in which that country is located. The world regions are: 1--North America, 2--Africa, 3 and 4--Europe, 5--South and Central America, 6--South Pacific, 7--Union of Soviet Socialist Republics (U.S.S.R.), 8--Far East, 9--Middle East and South-East Asia.

Note 1. KP2 is not used in first or second stage outpulsing when calling any country in the IDDD network.

Note 2. Public telephones are interfaced to TSPS (Traffic Service Position System). If you call an 800 number and whistle off using 2600 Hz, the distant toll office sends a wink back signal (a short on-hook) indicating it is ready to receive pulsing. TSPS responds to this wink back by printing out the original number called, the number called from, and the number MFed after the wink back. This print out goes to the billing and security departments.

PAIRED COUNTRY CODES

This is a list of paired country codes for use in first stage outpulsing on overseas calls. For two digit country codes simply add a zero. Example: The country code for England is 44. The paired country code is 044. Paired country codes that cannot be derived by this simple method are listed below.

Country	Country Code	Paired Code
Algeria	213	013
American Samoa	684	284
Bahrain	973	073
Belize	501	111
Bolivia	591	991
Brune	773	180
Cameroon	237	077
Costa Rica	506	806
Cyprus	357	087
Ecuador	593	293
El Salvador	503	003
Ethiopia	251	059
Fiji	679	879
Finland	358	088
French Antilles	596	896
French Polynesia (Tahiti)	689	289

Gabon	241	025
Gibralter	350	050
Guam	671	067
Guatemala	502	022
Guyana	592	892
Haiti	509	887
Honduras	504	884
Hong Kong	852	692
Iceland	354	854
Iraq	964	294
Ireland	353	083
Israel	972	072
Ivory Coast	225	285
Jordan	962	282
Kenya	254	074
Kuwait	965	015
Lesotho	266	186
Liberia	231	851
Libya	218	018
Luxembourg	352	292
Malawi	265	096
Marisat Atlantic	871	101
Marisat Pacific	872	102
Marisat Indian Ocean	873	103
Morocco	212	012
Namibia	264	194
Netherlands Antilles	599	099
New Caledonia	687	287
Nicaragua	505	975
Nigeria	234	014
Oman	968	068
Panama	507	247
Papua New Quinea	675	875
Paraquay	595	295
Portugal	351	281
Qatar	974	174
Saipan	670	071
Saudi Arabia	966	990
Senegal	221	021
St. Pierre/Miguelon	508	104
Suriname	597	097
Swaziland	268	168
Taiwan	886	006
Tanzania	255	075
Tunisia	216	016
Uganda	256	876
United Arab Emirates	971	291
Uruguay	598	288

USSR	7	007
Yemen Arab Republic	967	297
Zambia	260	008
Zimbabwe (Rodisia)	263	283

Notes: The Marisat codes are used when calling ships directly. Single stage outpulsing is used for calls to Mexico in this format: KP-180-City Code-digits-ST. To call an inward operator in Mexico use KP-190-City Code-09-ST. For directory assistance use KP-190-City Code-01-ST.

Red Boxing

Red boxing consists of simulating the tones produced when coins are deposited in a pay phone. Coin tones are beeps of 2200 Hz + 1700 Hz as follows:

5 cents - 1 beep, 66 milliseconds duration.

10 cents - 2 beeps, each 66 milliseconds duration with 66 millisecond pause between beeps.

25 cents - 5 beeps, each 33 milliseconds duration with a 33 millisecond pause between beeps.

Two methods have commonly been used by phone phreaks to produce these tones and make free calls.

1. The traditional Red Box consisting of a pair of Wien-bridge oscillators with the timing controlled by 555 timer chips.

2. Producing the signals with a computer which are recorded and then played back into the mouth piece of a pay phone.

A third very novel method has recently appeared. A phreak in the Midwest has extensively tested a method of red boxing which uses nothing more than a pair of brass or aluminum whistles. The whistles are 1/4 inch in diameter by 4 inches long and are tuned by means of a wooden dowel rod which fits snugly inside. The whistles can be brought precisely on frequency by tuning them against a known signal source such as a computer capable of producing the tones. Once tuned, the whistles are glued or taped together so they can be blown together to produce the dual tone used in coin signaling. It has been tested and proven that with a little practice these whistles can be used to make free calls. Now you can blow your money without spending a cent.

Black Boxes

Like blue boxes, black boxes got their name from the color of the first one found. The black box, also known as a mute, is a device which permits a subscriber to receive incoming long distance calls without charge to the calling party. This

information is presented mainly for its historical interest since black boxes will not work on the new electronic switching systems (ESS).

The construction and use of a black box was quite simple. A resistor of about 5600 ohms was connected in series with one side of the phone line. Connected in parallel across the resistor were a .47 mfd capacitor and a single pole single throw toggle switch. A momentary contact push button was connected across the line ahead of the other components for the purpose of briefly shorting the line. While waiting for an incomming call, the switch was left in the "on" position which shorted out the resistor and left the phone connected to the line as usual. When a call was received, the proceedure was to throw the switch, lift the receiver and push the button for a period less than one second. That brief short simulated taking the receiver off hook, which stopped the phone from ringing. Releasing the button simulated placing the receiver back on hook. Keep in mind that the receiver is really "off hook", but the presence of the resistor in series with the line reduces the current drawn by the phone below the level needed by telephone company equipment to detect the "off hook" condition. The capacitor bypassed the resistor for audio signals permitting normal conversation to take place. All the billing equipment knew was that a toll call was placed and the called party picked up the receiver and replaced it in less than one second. Since calls of less than one second duration are not billed, there was no charge for the call.

Later models of the black box featured diodes to automatically perform the button pushing and switch funtions. Aside from this refinement, they worked the same as the one described.

Cheese Boxes

The first divice of this kind was found in a cheese box, thus the name. A cheese box is a call diverter. Calls placed to one number are rerouted to another. This requires two phone lines each with its own number. Both lines terminate at the same location, ususally a vacant apartment or the apartment of an elderly widow. Only the first number is given out. When this number is called, the cheese box connects the first line to the second. The call is then answered on the second line at a location far removed from the cheese box.

This has been a favorite trick amoung bookies. Law enforcement officers trace the calls to the location of the cheese box and stage raids. When they get to the location all they find is an empty apartment or a confused old lady. Sometimes, realizing a cheese box is being used, they make a search for it. They don't always find the cheese box even though they know what they are looking for.

Early cheese boxes were quite simple consisting of only a few diodes and capacitors. They could be as small a fifty cent coin. Because of changes in the system, later models are more sofisticated.

Cheese boxes are in use today. They have been advertized in a national magazine. Apparently the device is not illegal unless put to an illegal use.

Silver Boxes

These devices are used by two people to talk or send computer data over long distance lines free of charge. A silver box is simply a normal tone pad with the

addition of four keys normally reserved for military or amateur radio use. These four additional keys are designated as follows:

A - Flash
B - Flash override priority
C - Priority communication
D - Priority override

Push button tone dialing uses a signaling method called Dual Tone Multifrequency or DTMF for short. It is a method of representing digits by playing two tones together using different tones for different digits. The following table lists the frequencies used by a tone pad including the signals of the silver box. All frequencies are in Hertz.

Tone Dialing Frequencies

LOW TONE GROUP (HZ)	HIGH TONE GROUP (HZ)			
	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Silver boxes can be made by modifying an existing key pad or they can be built up from a readily available tone encoder integrated circuit chip. The tones used can also be produced by many personal computers.

Making Free Calls with a Silver Box.

Silver boxes are used to seize long distance directory assistance lines. Two people calling at about the same time dial directory assistance for a selected area code. Not all area codes work for this. Those in the midwest seem to be favored. When the number rings, the "D" key is pressed. The caller will hear a pulsing tone. The first caller presses "6" on his keypad and waits. The second caller, following the same proceedure to this point, presses "7" on his key pad. The two are instantly connected. Those who have experimented with this say it doesn't matter wether the "6" or the "7" is pressed first so long as one caller uses "6" and the other "7".

Because of the necessity of prearranging the time of a silver box call, this method hasn't really caught on except as a fun experiment amoung advanced phone phreaks.