Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db227

Title	**Telephone hackers beware: The phone company is cracking down on you**
Publication	*The Tech (MIT)*
Date	1972-10-27
Author(s)	Eleccion, Marce
Abstract	Reprint of an article by Marce Eleccion which appeared in IEEE Spectrum in August, 1972 (db228). Intro says that the recent arrest of an unnamed MIT student (presumably Stephen Owades) has aroused interest in what constitutes toll fraud. See db213.
Keywords	MIT; Stephen Owades; blue box
Notes	Also in MISC01-006 as part of Harvard/MIT research

Telephone hackers beware

*The recent arrest of an MIT student for "fraud by wire" or phone hacking (*The Tech *October 17) has arroused a great deal of interest in the MIT community as to what is and what is not phone fraud; and what Telco intends to to about it. The following article, which appeared in the August 1972 edition of* IEEE Spectrum *is authoritative and informative. It is reprinted here by permission. – Editor)*

By Marce Eleccion
Staff Writer, *IEEE Spectrum*

As if the telephone utilities didn't have enough to worry about, it seems that a new breed of defrauder has emerged over the past decade to intrude upon a particularly vital part of the telephone system – the toll network. Armed with hardware that ranges from the shoddiest of devices to the newest in integrated circuitry, these "phone phreaks" are able to call virtually around the world via the telephone network, without paying. The methods that are currently being used exploit an unfortunate vulnerability that exists in the present toll dialing telephone system: the inclusion of control signaling within the voice-frequency band.

What is basically causing concern among the telephone utilities is the fact that the single frequency (SF) and multifrequency (MF) toll-traffic signalling tones, which are presently being carried within the voice transmission band, can be generated directly from the more than 100 million telephone instruments within the easy grasp of practically the entire US populace. Although the economic and technological considerations that led to the eventual decision to install such a system a few decades ago may have been justified at the time, telephone companies are now beginning to regret ever having opted for such an obviously fallible method of toll signalling.

The problem of course arises when individuals out to beat the phone system attempt to initiate SF and MF signalling on their own, thus preempting the roll of the toll operator who normally directs these network control signals. The device that these defrauders (who, like most criminal elements, represent only a small percentage of the population) use is called a "blue box," supposedly because the first such unit discovered was that color. Essentially a tone generator, the blue box has been found in all forms, shapes, and disguises (some even designed to self-destruct). The only unit that this writer has seen (at AT&T) was clandestinely constructed in a Navy shipyard and represented magnificent craftsmanship on the part of the builder – a somewhat dubious tribute to the ingenuity of some of these phone defrauders.

Actually, this type of phone phreak – the MFer or blue-boxer – belongs to a larger category of phone defrauders, all practitioners in the art of "ripping off" the phone companies. In the recent literature publicizing these "phone phrauds" (a more accurate epithet), the implication is that they are a loosely organized but glamorous camaraderie. Nothing could be further from the truth. Rather than the anti-establishment avant-garde these defrauders pretend to be, they are is essence violaters of the public faith, since their crime is directed at the telephone community as a whole – the user as well as the carrier.

Certainly, such sobriquets as Captain Crunch, Dr. No, the Snark, and Midnight Skulker contribute a colorful image to these supposed modern day Robin Hoods. When one considers the fate that befalls them, however, the color begins to fade. Captain Crunch (derived from the whistle found in the breakfast cereal of the same name that generated 2600 Hz, a traffic signalling tone), one of the original phone phrauds, was recently arrested by the FBI and faces prosecution under Federal statues. Individuals said to have built fraud devices for elements of organized crime have either disappeared or died violently – a serious deterrent to those contemplating making such devices for others.

The extent of phone defrauding

Although the increase of phone fraud since 1965 has been estimated as high as 700 percent, there are indications that the phone companies are beginning to win the battle against offenders, mainly because of an aggresive toll-fraud program they were wise enough to institute early in 1971 and the development of highly effective and sophisticated detection techniques.

In the area of fraudulent credit-card and third-number calls (billings to a third number at the calling party's request), the Bell System has succeeded in halting a spiraling trend in revenue losses, as can be seen in the following:

Credit-card and Third-number Fraud

Year	*Amount*
1968	$3.5 million
1969	6.9 million
1970	28.3 million
1971	22.2 million

Not only were revenue losses appreciably reduced in 1971, but there was a marked increase in prosecution – 330 arrests and 255 convicitons (with many cases still pending in the courts) – as compated with 215 arrests and 207 convictions in 1970.

Another area where losses have been substantially reduced is coin telephone larceny. In 1967, Bell System losses from this type of crime reached an all-time peak of $3.5 million, which includes equipment damage and destruction. By 1971, these types of losses were reduced to about $2 million, which was largely due to widespread use of armored coin telephones with sophisticated locks, metal-clad cables, heavy-duty dials and handsets, and single-slot coin telephones that detect and resist "stuffing" as well as slugs.

Unfortunately, the losses th
are sustained due to blue-b
toll frauds are difficult to es
mate. Bell representitives ha
been quoted at a conservati
figure of between $50,000 a
$100,000 a year, but indepe
dent telephone company rep
sentitives give estimates as hi
as $150 million. The arrest a
conviction record is a little mo
encouraging; although the
were only six arrests and tw
convictions in 1970, there we
45 arrests and 35 convictio
(cases still pending) in 1971.

Although the extent of blu
box activities has been thoug
to be somewhat restricted, t
recent experience of a few Be
Laboratories investigators ma
prove to be a more accura
indicator of the numbers th
are actually involved. In visit
a large eastern engineer
school [*unnamed in the artic*
to query three students wh
were active MFers, the Be
group was informed that appro
imately 100 blue-box devic
were in use at this one scho
alone.

If one can believe the liter
ture, the ramifications of blu
boxing exceed the ability to ju
make free calls. According to
least one source, phone phrau
are also able to intrude upon th
privacy of time-shared comput
banks that are accessed throug
the common carriers. In queryi
the director of engineering of
major software corporation, th
writer was informed that it
indeed possible to do so, esp
cially if one learns the contr
format of a particular system
a former or present user of th
computing service. Howeve
even if an intruder is able
breach the top two levels
security, there are additional le
els within the file system itse
that are known only to the us
himself, making it an exceedi
ly difficult feat to achieve actu
intrusion. As if that weren
enough, truly critical data can
stored in a scrambled forma

The phone company is cracking down on you

with the chances of deciphering the algorithm scheme virtually nonexistent.

Given the undaunted spirit of a resourceful intruder, however, it is feasible that he will continue his attempts at cracking the code. If this happens, the abnormal access condition is easily detected by error-signal analysis and corrective measures may be taken by the computer firm. In addition, any line access to a computer port must be accompanied by suitable signaling conditions or it will be shut off; hence a phone phraud must also be in possession of expensive data equipment. Of course, the use of leased lines and full dedicated file areas pre-empts any nonphysical access to a computer bank.

Another blue-box intrusion that has been reported is that of wire tapping. The truth of this claim seems to be in doubt, ever, although it is possible for a verification operator using a verification trunk to intrude upon a subscribers phone conversation in an emergency, a situation which many readers may have experienced.

Other blue-box variations that have been speculated upon include the more expensive telephone-answering devices that can be queried for messages remotely by the user after signalling with a tone blast. Without direct information, however, the chances of selecting a single multifrequency tone from the telephone transmission bandwidth of 200-3200 Hz are pretty slim.

Detection, apprehension and prosecution

Not suprisingly, the detection methods that are being employed by the telephone companies are not being divulged to the general public (this writer included) An area of obvious great importance, the detection of any criminal activity is dependent on many factors: defrauder error, suspicion based on calculated hunches or calling patterns, billing analysis, or even informants.

Specific and extremely specialized equipment may also be used, such as that need for SF/MF detection on a telephone line. What this device does is detect the presence of an unusually long burst of 2600 Hz on a line and trip a counter that records the length of the call, as well as other data. Such data might include date and time, the legitimate toll number that is dialed (usually a charge-free number), the SF and MF signals illegally entered onto the line, and the conclusion of the call.

According to Bell Labs experts, the SF/MF method of evidence gathering is only one of a great number of detection tools that are at the disposal of security and law enforcement agencies, with many techniques displaying a high level of sophistication.

The countermeasures problem confronting today's telephone utility are enormous, especially with the increased availability of modern electronics gadgetry. Tom Powers of Bell Labs has summed it up in this way:

"Whenever information as to how a system is intended to work comes out in any fashion, a few people very quickly find a way around it. It seems that, no matter how smart we are, it doesn't take long until someone figures out a way to break the code and the losses start going up again . . . We're very much concerned about tipping our hand and giving away the combination to the safe."

The temptation to defeat the phone system at this counter-countermeasure game may seem irresistable to some; if so, theu would be wise to consider both the penalties that must be exacted and the undaunted resolution of the phone companies. Joe F. Doherty, director of corporate security for AT&T has stated his position in prosecuting phone defrauders most unequivocally:

"We are prosecuting aggressively and without any exception. We have a federal felony statue, we would like felony laws in every state, in addition to existing laws that make fraud a violation that is other than just a misdemeanor . . . We're getting more interest out of the FBI and we're getting more felony prosecutions. So when these people are convicted of a Federal felony, they've got the stigma for

What Doherty was referring to was Title 18 of the US Code, specifically paragraph 1343 entitled "Fraud by Wire, Radio or Television." The wording of the pertinent sections of this statue may seem like legalese to some, but the meaning of the penalties for those prosecuted for this type of fraud come through loud and clear – a fine of "not more than $1000," imprisonment for "not more than five years," or both.

Concerning the actual printing of written material advocating (as some of the nonconformist magazines and underground newspapers have been doing with increasing frequency) the defrauding of telephone companies, the statues that have been passed in California, Georgia, Kansas, Maryland, and Virginia (Gov. Rockefeller recently vetoed a similar law in New York) prohibiting this are expected to be court tested within the next few months. Organizations that advocate similar disruption of the telephone system will probably fall under this jurisdiction.

The Solution

This examination of the telephone defrauding problem has turned up various answers – some of which may very neatly apply to the general problem of system defrauding. Aside from specific, short-term solutions, such as the installation of tamper-proof phones and the implementation of detection devices to monitor the illegal use of telephone traffic signalling, any long-term solution must be approached from three vantage points: those of the carrier, the user, and the Government.

From the point of view of the telephone system itself, it seems imperative for the system designer – the engineer – to examine the societal implications as well as the cost-benefit factors. Certainly the present blue-box dilemma would not have arisen if the system designer had not included traffic signalling within the voice-frequency band, thus inviting fraud. On the other hand, there will always be the there will always be the temptation to "beat the system" no matter what its degree of sophistication. So the engineer must choose the right tradeoffs between system complexity and user cost, and system vulnerability and system cost.

For the user, the "solution" to system defrauding of any type lies in greater moral responsibility. Rampant anti-establishment feeling must be partly to blame (although personal gain should not be discounted as part of the defraud "psyche").

The Government's role in halting telephone fraud has been one of vigorous apprehension and their strong desire to act as witnesses for the prosecution.

In the face of such a three-pronged assault, there is good reason to expect a victory in the war against the "blue box bandits."