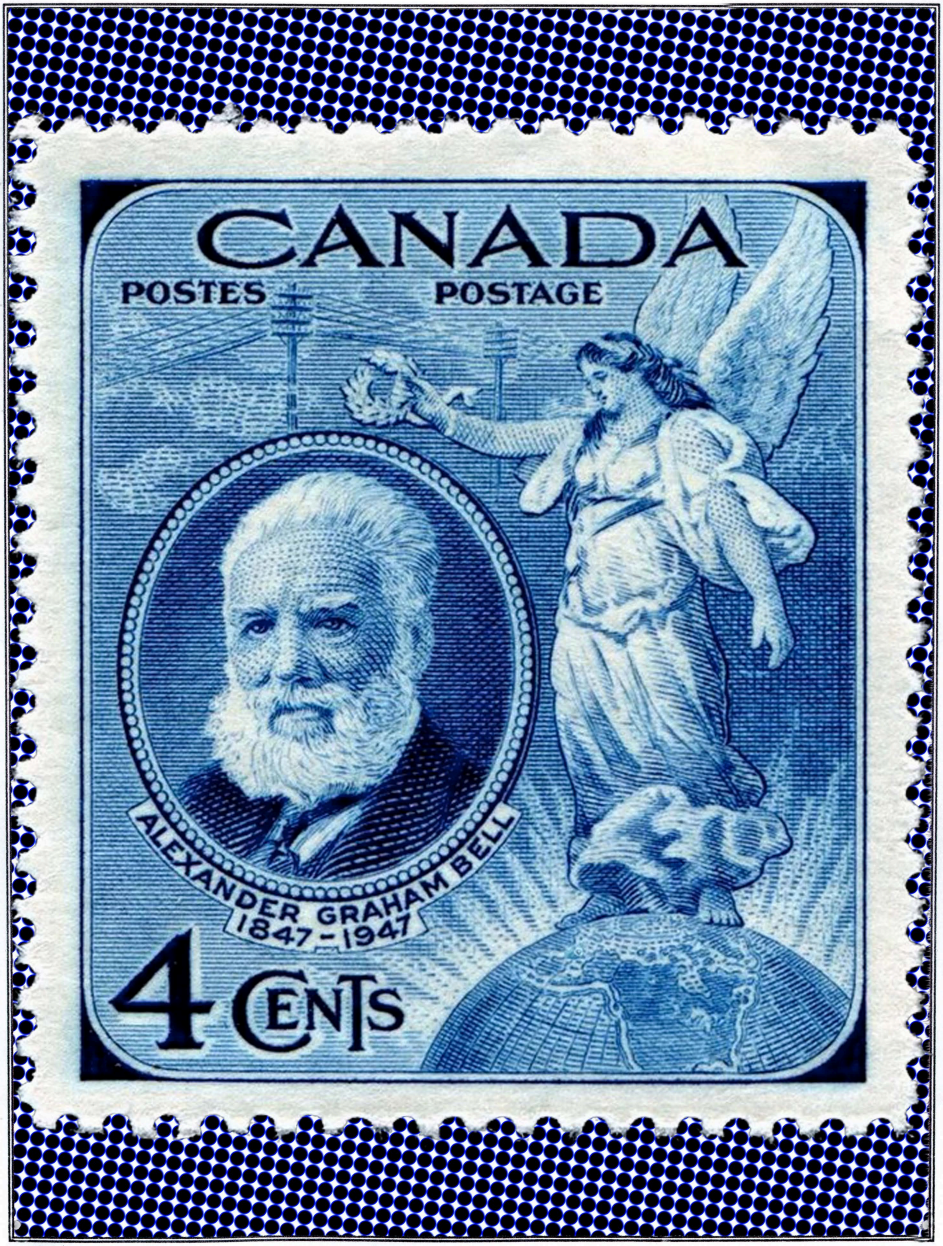
2600

The Hacker Digest - Volume 7

1990



FORMAT

The 1990 cover format was pretty much identical to that of 1989. A price of $4 appeared on the Autumn cover while the Winter issue was designated as "Winter, 1990" on the cover instead of "Winter, 1990-91" which had been the format followed in previous years (and which was followed in the page footers of this issue).

The page length remained at 48 pages and followed the same page numbering scheme as in 1989 with covers and inside covers not labeled with page numbers. Color appeared on the front and back covers but not on the insides. The table of contents continued to appear on the back cover, continuing the tradition of a unique title for each issue - Spring: "take a look"; Summer: "ingredients"; Autumn: "within..."; and Winter: "internal organs". A dashed line continued to surround article titles in the contents. Second class postage permit info was printed on the back covers of the Spring and Autumn issues only.

Messages continued to be hidden in tiny print in the space on the back cover where a mailing label would go, continuing another tradition - Spring: "$LOD^2 < 1300$" (a good-natured ribbing of the hacker group Legion of Doom, basically saying that LOD squared was less than *2600* divided in half); Summer: "do it" (a call for action of some sort - in print that was almost impossible to see); Autumn: "the threat is real" (a not-so-coded warning to the hacker community, as if the events of the year so far weren't enough warning); and Winter: "u.s. vs. us" (a lined up series of letters that spelled out how we felt about recent governmental actions against hackers).

COVERS

All of this year's covers were drawn by Holly Kaufman Spruch. The mini-covers would again continue throughout the year. Each of this year's covers focused on events in the tumultuous hacker world.

Spring 1990 focused on the aftermath of a massive series of raids that shocked and traumatized the entire hacker community. The hacker newsletter *Phrack* was shut down, many arrests were made, and the future looked bleak. The setting for this cover is the inside of a dance hall, where five guys are standing in various baseball uniforms, each representing one of the cities in the vicinity of the raids: New York, Chicago, Atlanta, St. Louis, and Houston. Surveillance cameras are everywhere, marked with the insignia "For Your Protection," which was also the title of this issue's eight page editorial, which pretty much summed up the whole sordid story. A security guard aims a gun at our suspects, with the insignia of "F.Y.P." on his shirt. A message scrolling on the wall reads: "Come In Number 2599, Your Time Is Up....." This is a reference to a Pink Floyd song as well as an expression of concern, as it was widely feared that our number was coming up next. "Acid House" is scrawled on the wall, a reference to the genre of music, but since there's a camera in the way, it could also read "Acid's House," a reference

to a local hacker and *2600* contributor named Acid Phreak, whose home had also been raided. There is a door labeled "Exit or Entrance" with a foot in it. Someone is either about to enter or leave. The future was uncertain. The mini-cover has the phrase "The Whole World's Watching," an iconic chant from antiwar protesters in Chicago back in 1968, but also a message to current-day authorities that their actions were being scrutinized.

The Summer 1990 cover shows a busy street scene, where protesters are confronting a tank, very much in the style of the Tiananmen Square scene one year earlier. Driving the tank is a man with a chef's hat, a clear reference to Assistant United States Attorney William Cook, who led the prosecution against *Phrack* publisher Craig Neidorf. The tank has the words "Born Criminals" written on it. Whether that's referring to the people who drive this tank or the people the tank is targeting remains unclear. The tank seems to be guarding a locked door marked with the letters "INT." The first few letters are blocked, but it could easily represent a Sprint building housing various secrets of interest to hackers. We also see a trio of kids on skateboards, riding freely in the distance. This symbolized hope and the future, as well as paralleling the demonization of skateboarders in the eyes of society, who were often persecuted in similar ways as hackers. The bus leaving the scene symbolized the founding of the Electronic Frontier Foundation (established as a direct result of the raids that started the year) and their perceived abandoning of their hacker connections once they began operations. As one of the EFF founders was also a Grateful Dead lyricist, the quote on the bus reading "all a friend can say is ain't it a shame" seemed appropriate. The mini-cover is a symbol that was known to evangelical anti-rock crusaders as a "secret Satanic symbol." It really wasn't, but we wanted to stir things up a bit.

Autumn 1990 features a television set showing a crowd of people in a theater watching a movie showing a guy looking at a computer screen. On the computer screen are the words "Never Erase The Past" written over an Iraqi flag. Military action in the Gulf was on the horizon and it seemed as if the world was on the verge of forgetting the mistakes of the past and repeating them in the near future. A gloved hand appears ready to unplug the entire image. In the mini-cover, a weeping Macintosh icon appears next to George Washington's image from a dollar bill. This was a reference to yet another FBI action against computer users, this time as they were investigating a group called the Nu Prometheus League, which had allegedly gotten access to and distributed some of the highly secret Macintosh source code. More innocent people who had nothing to do with this, including people involved in the founding of EFF, were subjected to questioning. We felt that George Washington wouldn't have been pleased.

For Winter 1990, we had another cover featuring a computer, this one room-sized with three people standing on the keyboard. The first character is completely unarmed, the second is threatening the first with a club, and the third is threatening the second with a gun. Meanwhile, the third character has a tank and an airplane dropping bombs in his immediate vicinity. This represented the growing danger within the hacker world, as one entity seemed to always have a bigger one behind it that was really calling the shots. Of course, this also paralleled with what was going on in the world with the calls

for war in the Middle East. Interestingly, and for reasons unknown, the entire image appears to be taped onto a blue wall. The mini-cover is also a bit mysterious, with part of a map of Cuba appearing, along with Arabic writing that translated to "In the name of God, the Most Gracious, the Most Merciful," and a 43-digit long, seemingly random, sequence (4197169399375105820974944592307816406286208), which was actually 43 digits of Pi (starting with the 36th, running through the 78th. To one of the many agencies monitoring us, it might have seemed like a code of some sort. There were no search engines back then to quickly look this sort of thing up, so unless they actually tried to calculate Pi or had a listing lying around, they most likely would have wasted a lot of time trying to figure this out.

INSIDE

The staff section retained credits for Editor-In-Chief, Artwork, Design, Writers, and Remote Observations (the latter correcting 1989's spelling mistake). A new credit for Photo Salvation was added. The Writer list ended with "the faithful anonymous bunch" for Spring and Summer, "the unusual anonymous bunch" for Autumn, and "the anonymous many" for Winter. The Design and Photo Salvation credits were removed in Autumn, the same issue where we launched Shout Outs. (It should be noted from the Shout Out section that Steve was our old printer and Franklin was our new laser printer.) The staff section grew bigger in Autumn and wound up bigger still and back on page 3 for Winter. In that issue the Editor-In-Chief credit was shared with "Alan Smithee," which is the traditional name used by film directors wanting to disown a project. We can't comment on what it meant in this case, especially since the name was shared with the actual editor.

Mailing info continued to be printed on page 3 as required by the post office. A new line was added in the Spring issue for "NETWORK ADDRESSES" which contained two methods of sending us email in the very early days of the Internet. That was reduced to one address in the Summer issue. The Autumn issue showed an addition of "(U.S. funds)" next to our prices, as we were getting all sorts of foreign checks and money orders our bank had no idea how to process.

Apart from our own house ads, we had stopped accepting advertising at this point outside of the *2600* Marketplace, which continued to appear on page 41.

The Spring issue saw the coming of our biggest story yet, a massive nationwide crackdown on hackers which would eventually lead to the founding of the Electronic Frontier Foundation. Operation Sundevil was a major part of this, but there were other raids going on at the same time and the sense of fear and doom in the hacker world was palpable. We launched the year with a massive eight page editorial that outlined everything going on, how it all related, and what the threat was. It was put online and reposted globally, making it one of our most read pieces ever - and gaining a ton of media and mainstream attention. We saw the writing on the wall: "Censorship, clampdowns, 'voluntary' urine tests, lie detectors, handwriting analysis, surveillance cameras, exaggerat-

ed crises that invariably lead to curtailed freedoms....” The hacker group known as the Legion of Doom was raided and effectively shut down. A popular BBS known as The Phoenix Project was seized, along with more than a dozen others. A completely uninvolved company (Steve Jackson Games) was also raided and nearly put out of business simply because one of their employees had used that BBS. A hacker newsletter known as *Phrack* was shut down as a result of one of the raids, leading many to realize that electronic publishing wasn't protected in the same way as traditional paper publishers such as *2600*. We knew it could go one of two ways: either freedom of the press would be applied to *all* press or we could very well be next as rights became further eroded.

This wasn't that different from what we had seen before with the persecution of hackers. We were pretty used to it. “Who would you target as the biggest potential roadblock if not the people who *understand* the technology at work?” The distinction here was the sheer number of people now being affected. And that was what started to get attention. We drew parallels to other eras and places: “The words and ideas are easily translatable to any time and any culture.”

The words “we've come face to face with a very critical moment in history” were not an exaggeration. The school email accounts of the *Phrack* editors were being monitored by the authorities, an unprecedented move at the time. Massive amounts of private email stored on the seized BBSes were being read, in apparent violation of the Electronic Communications Privacy Act. But what was probably the most blatant example of the abuse of power being set loose here was the declaration that a leaked document published in *Phrack* was worth $79,449. (We decided to have some fun with that and offer copies for $20,000 less in our pages.) In addition to the dangerous precedent of punishing a publisher for leaked documents that came into their possession, the declaration turned out to be an outright lie: the document could be obtained legally for only $13, a fact that came out at the trial later in the year, thanks to a whistleblower who had become aware of what was going on through the massive campaign we were involved in. One positive thing that came from all of this was that we learned the power of electronic communications in getting the word out on the Neidorf case.

The charges were dropped in the middle of the trial, leaving *Phrack* publisher Craig Neidorf vindicated but heavily in debt due to the legal expense. The impression that the newly formed EFF would be a hacker legal defense fund turned out not to be the case and there seemed to be an attempt to distance themselves from hackers in those early days, much to the hacker community's consternation.

Needless to say, our perspective was not the only one on the subject and we devoted a bit of space to some of the criticism we were getting for taking the stand we did. We also got a good bit of critique from members of the hacker community who took umbrage at our talking to the media at all, thinking no good could possibly come from it. Our position was that we had to get the word out somehow - and that this was worth taking a chance on a reporter getting the message. We had some successes and that was enough to want to keep going.

The *2600* meetings expanded to San Francisco in 1990. We also had a bit of fun at the New York meeting when we discovered we were under surveillance, a fact later admitted to by the New York State Police. Needless to say, pictures were printed.

Payphone photos were now a regular feature on the inside front cover. *2600* BBSes, however, had become a thing of the past. We saw touch tone fees start to be eliminated and the term "slamming" was used for the first time. Robert Morris was sentenced to a fine and probation for accidentally unleashing the Internet worm back in 1988. An article on COCOTs (Customer Owned Coin Operated Telephones) in the Summer issue drew lots of attention, both positive and negative. This was also the case for an article in the Autumn issue that revealed a credit card algorithm. Critics who felt the only possible purpose for this was to help in credit card fraud were rebuffed by a letter expressing gratitude from a credit card processing office that now had a way to verify numbers free of charge. The Autumn issue also saw a milestone: the plans for converting a Radio Shack tone dialer into a red box. This would prove to be a major pain in the ass for phone companies for many years to come. Interestingly enough, when a reader first suggested the idea of converting a tone dialer into a red box, we dismissed it, saying "there wouldn't be much point." Fortunately, more enlightened heads prevailed.

As the year closed, GTE was on the verge of becoming the nation's largest phone company after acquiring Contel. Caller ID was getting more prevalent, and phone companies everywhere were fighting the option that allowed callers to block their numbers from being sent. Bulgaria had become a breeding ground for computer viruses and BellSouth became the first Regional Bell Operating Company to go completely electronic. There were calls for more magazines like *2600* and, in the wake of all of the raids, *we* were calling for more BBSes: "The need for public hacker boards has never been greater."

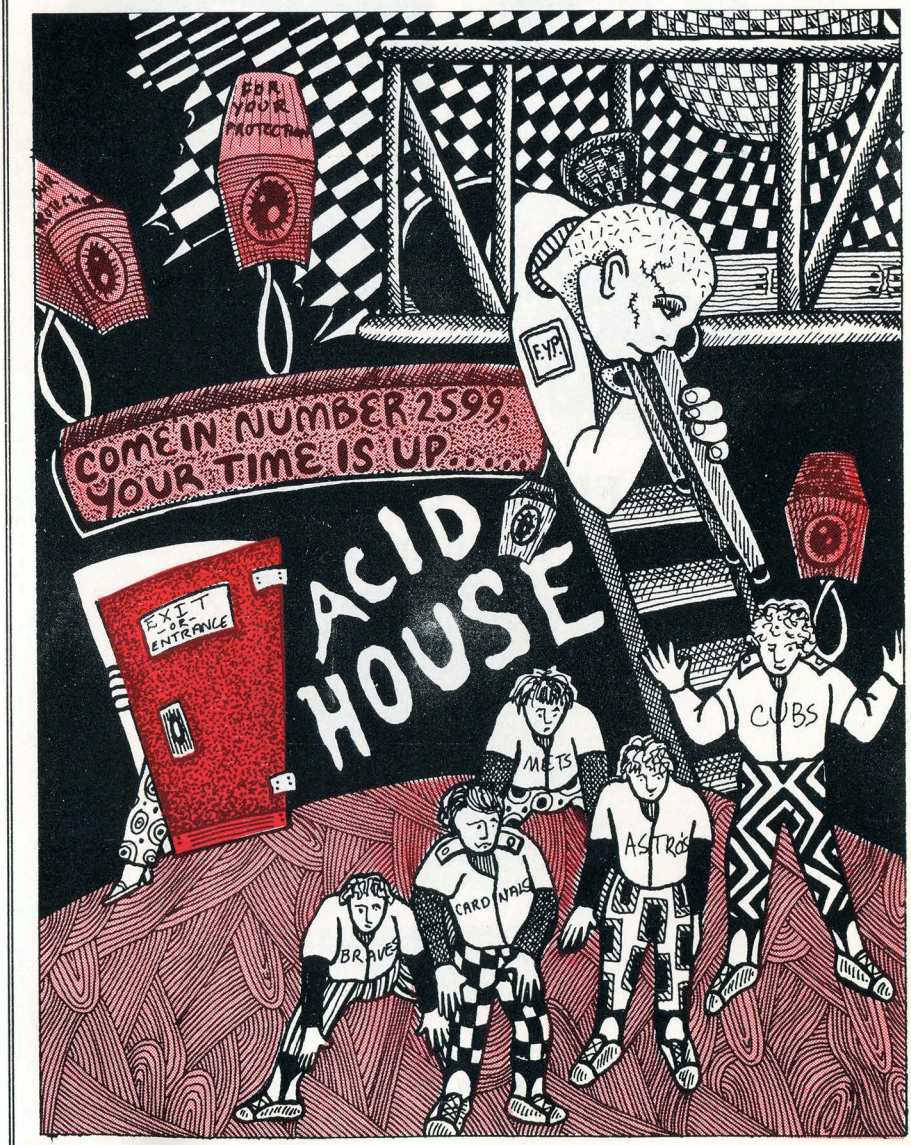
Overall, it was a turbulent year, with a fair amount of leaks getting printed and lots of talk of privacy, wiretaps, and the like. Throughout it all, we tried to maintain a feeling of hope by emphasizing: "Technology in the hands of imaginative people can do wonderful things." We had seen quite a bit of the flipside already.

2600

The Hacker Quarterly

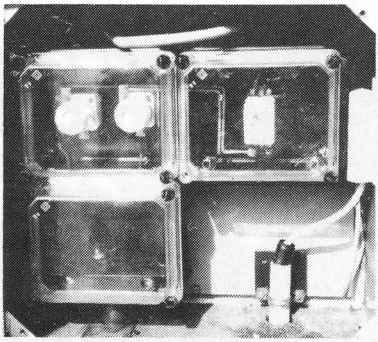
The Whole World's Watching

VOLUME SEVEN, NUMBER ONE!
SPRING, 1990



NAKED DUTCH PAYPHONES

In the streets of Amsterdam



AND A FULLY CLOTHED ONE

In Australia

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1990, 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESSES: 2600@well.sf.ca.us, 2600@dasys1.UUCP.

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

FOR YOUR PROTECTION

A year ago, we told the stories of Kevin Mitnick and Herbert Zinn, two hackers who had been sent to prison. It was then, and still is today, a very disturbing chain of events: mischief makers and explorers imprisoned for playing with the wrong toys and for asking too many questions. We said at the time that it was important for all hackers to stand up to such gross injustices. After all, they couldn't lock us all up.

It now appears that such an endeavor may indeed be on the agendas of some very powerful U.S. governmental agencies. And even more frightening is the realization that these agencies don't particularly care who or what gets swept up along with the hackers, as long as all of the hackers get swept up. Apparently, we're considered even more of a threat than we had previously supposed.

In retrospect, this doesn't come as a great deal of a surprise. In fact, it now seems to make all too much sense. You no longer have to be paranoid or of a particular political mindset to point to the many parallels that we've all been witnesses to. Censorship, clampdowns, "voluntary" urine tests, lie detectors, handwriting analysis, surveillance cameras, exaggerated crises that invariably lead to curtailed freedoms.... All of this together with the overall view that if you're innocent, you've got nothing to hide. And all made so much more effective through the magic of high tech. Who would *you* target as the biggest potential roadblock if not the people who *understand* the technology at work? It appears the biggest threats to the system are those capable of manipulating it.

What we're about to tell you is frightening, plain and simple. You don't have to be a hacker to understand this. The words and ideas are easily translatable to any time and any culture.

Crackdown

"We can now expect a crackdown...I just hope that I can pull through this one and that my friends can also. This is the time to watch yourself. No matter what you are into.... Apparently the government has seen the last straw in their point of view.... I think they are going after all the 'teachers'...and so that is where their ener-

gies will be put: to stop *all* hackers, and stop people *before* they can become threats."

This was one of the reactions on a computer bulletin board to a series of raids on hackers, raids that had started in 1989 and spread rapidly into early 1990. Atlanta, St. Louis, and New York were major targets in what was then an undetermined investigation.

This in itself wouldn't have been especially alarming, since raids on hackers can almost be defined as commonplace. But this one was different. For the very first time, a hacker newsletter had also been shut down.

Phrack was an electronic newsletter published out of St. Louis and distributed worldwide. It dealt with hacker and phone phreak matters and could be found on nearly all hacker bulletin boards. While dealing with sensitive material, the editors were very careful not to publish anything illegal (credit card numbers, passwords, Sprint codes, etc.). We described "Phrack World News" (a regular column of *Phrack*) in our Summer 1989 edition as "a must-read for many hackers". In many ways *Phrack* resembled *2600*, with the exception of being sent via electronic mail instead of U.S. Mail. That distinction would prove to be *Phrack*'s undoing.

"Apparently, we're considered even more of a threat than we had previously supposed."

It now turns out that all incoming and outgoing electronic mail used by *Phrack* was being monitored by the authorities. Every piece of mail going in and every piece of mail coming out. These were not pirated mailboxes that were being used by a couple of hackers. These had been obtained legally through the school the two *Phrack* editors were attending. Privacy on such mailboxes, though not guaranteed, could always be assumed. Never again.

It's fairly obvious that none of this would have happened, none of this *could* have happened had *Phrack* been a non-electronic magazine. A printed magazine would not be intimidated into giving up its mailing list as *Phrack* was. Had a printed magazine been shut down in this fashion after having all of their mail opened and read, even the most thick-headed sensationalist media types would have caught on: hey, isn't that a violation of the First Amendment?

Those media people who understood what was happening and saw the implications were very quickly drowned out in the hysteria that followed. Indictments were being handed out. Publisher/editor Craig Neidorf, known in the hacker world as Knight Lightning, was hit with a seven count indictment accusing him of participating in a scheme to steal information about the enhanced 911 system run by Bell South. Quickly, headlines screamed that hackers had broken into the 911 system and were interfering with emergency telephone calls to the police. One newspaper report said there were no indications that anyone had died or been injured as a result of the intrusions. What a relief. Too bad it wasn't true.

In actuality there have been very grievous injuries suffered as a result of these intrusions. The intrusions we're referring to are those of the government and the media. The injuries have been suffered by the defendants who will have great difficulty resuming normal lives even if all of this is forgotten tomorrow.

And if it's not forgotten, Craig Neidorf could go to jail for more than 30 years and be fined $122,000. And for what? Let's look at the indictment:

"It was... part of the scheme that defendant Neidorf, utilizing a computer at

OWN GOOD

the University of Missouri in Columbia, Missouri would and did receive a copy of the stolen E911 text file from defendant [Robert J.] Riggs [located in Atlanta and known in the hacker world as Prophet] through the Lockport [Illinois] computer bulletin board system through the use of an interstate computer data network.

"It was further part of the scheme that defendant Neidorf would and did edit and retype the E911 Practice text file at the request of the defendant Riggs in order to conceal the source of the E911 Practice text file and to prepare it for publication in a computer hacker newsletter.

"It was further part of the scheme that defendant Neidorf would and did transfer the stolen E911 Practice text file through the use of an interstate computer bulletin board system used by defendant Riggs in Lockport, Illinois.

"It was further part of the scheme that the defendants Riggs and Neidorf would publish information to other computer hackers which could be used to gain unauthorized access to emergency 911 computer systems in the United States and thereby disrupt or halt 911 service in portions of the United States."

Basically, Neidorf is being charged with *receiving* a stolen document. There is nothing anywhere in the indictment that even suggests he entered any computer illegally. So his crimes are receiving, editing, and transmitting.

Now what is contained in this document? Information about how to gain unauthorized access to, disrupt, or halt 911 service? Hardly. The document (erroneously referred to as "911 software" by the media which caused all kinds of misunderstandings) is quoted in *Phrack* Volume 2, Number 24 and makes for one of the dullest articles ever to appear in the newsletter. According to the indictment, the value of this 20k document is $79,449. **[See related story, page 37]**

Shortly after the indictments were handed down, a member of the Legion of Doom known as Erik Bloodaxe issued a public statement. "[A group of three hackers] ended up pulling files off [a Southern Bell system] for them to look at. This is usually standard procedure: you get on a system, look around for interesting text, buffer it, and maybe print it out for posterity. No member of LOD has ever (to my knowledge) broken into another system and used any information gained from it

"They are going after all the 'teachers'."

for personal gain of any kind...with the exception of maybe a big boost in his reputation around the underground. [A hacker] took the documentation to the system and wrote a file about it. There are actually two files, one is an overview, the other is a glossary. The information is hardly something anyone could possibly gain anything from except knowledge about how a certain aspect of the telephone company works."

He went on to say that Neidorf would have had no way of knowing whether or not the file contained proprietary information.

Prosecutors refused to say how hackers could benefit from the information, nor would they cite a motive or reveal any actual damage. In addition, it's widely speculated that much of this information is readily available as reference material.

In all of the indictments, the Legion of Doom is defined as *"a closely knit group of computer hackers involved in: a) disrupting telecommunications by entering computerized telephone switches and changing the routing on the circuits of the computerized switches; b) stealing proprietary computer source code and information from companies and individuals that owned the code and information; c)*

stealing and modifying credit information on individuals maintained in credit bureau computers; d) fraudulently obtaining money and property from companies by altering the computerized information used by the companies; e) disseminating information with respect to their methods of attacking computers to other computer hackers in an effort to avoid the focus of law enforcement agencies and telecommunication security experts."

Ironically, since the Legion of Doom *isn't* a closely knit group, it's unlikely that anyone will be able to defend the group's name against these charges — any defendants will naturally be preoccupied with their own defenses. (Incidentally, Neidorf was not a part of the Legion of Doom, nor was *Phrack* a publication of LOD, as has been reported.)

The Hunt Intensifies

After learning of the *Phrack* electronic mail surveillance, one of the system operators of *The Phoenix Project*, a computer bulletin board in Austin, Texas, decided to take action to protect the privacy of his users. "I will be adding a secure encryption routine into the e-mail in the next 2 weeks - I haven't decided exactly how to implement it, but it'll let two people exchange mail encrypted by a password only known to the two of them.... Anyway, I do not think I am due to be busted...I don't do anything but run a board. Still, there is that possibility. I assume that my lines are all tapped until proven otherwise. There is some question to the wisdom of leaving the board up at all, but I have personally phoned several government investigators and invited them to join us here on the board. If I begin to feel that the board is putting me in any kind of danger, I'll pull it down with no notice - I hope everyone understands. It looks like it's sweeps-time again for the feds. Let's hope all of us are still around in 6 months to talk about it."

"All incoming and outgoing electronic mail used by Phrack was being monitored by the authorities."

The new security was never implemented. *The Phoenix Project* was seized within days.

And the clampdown intensified still further. On March 1, the offices of Steve Jackson Games, a publishing company in Austin, were raided by the Secret Service. According to the Associated Press, the home of the managing editor was also searched. The police and Secret Service seized books, manuals, computers, technical equipment, and other documents. Agents also seized the final draft of a science fiction game written by the company. According to the *Austin American-Statesman*, the authorities were trying to determine whether the game was being used as a handbook for computer crime.

Callers to the *Illuminati* bulletin board (run by Steve Jackson Games), received the following message:

"Before the start of work on March 1, Steve Jackson Games was visited by agents of the United States Secret Service. They searched the building thoroughly, tore open several boxes in the warehouse, broke a few locks, and damaged a couple of filing cabinets (which we would gladly have let them examine, had they let us into the building), answered the phone discourteously at best, and confiscated some computer equipment, including the computer that the BBS was running on at the time.

"So far we have not received a clear explanation of what the Secret Service was looking for, what they expected to find, or much of anything else. We are fairly cer-

tain that Steve Jackson Games is not the target of whatever investigation is being conducted; in any case, we have done nothing illegal and have nothing whatsoever to hide. However, the equipment that was seized is apparently considered to be evidence in whatever they're investigating, so we aren't likely to get it back any time soon. It could be a month, it could be never.

"To minimize the possibility that this system will be confiscated as well, we have set it up to display this bulletin, and that's all. There is no message base at present. We apologize for the inconvenience, and we wish we dared do more than this."

Apparently, one of the system operators of *The Phoenix Project* was also affiliated with Steve Jackson Games. And that was all the authorities needed.

Raids continued throughout the country with reports of more than a dozen bulletin boards being shut down. In Atlanta, the papers reported that three local LOD hackers faced 40 years in prison and a $2 million fine.

Another statement from a Legion of Doom member (The Mentor, also a system operator of *The Phoenix Project*) attempted to explain the situation:

"LOD was formed to bring together the best minds from the computer underground - not to do any damage or for personal profit, but to share experiences and discuss computing. The group has *always* maintained the highest ethical standards.... On many occasions, we have acted to prevent abuse of systems.... I have known the people involved in this 911 case for many years, and there was *absolutely* no intent to interfere with or molest the 911 system in any manner. While we have occasionally entered a computer that we weren't supposed to be in, it is grounds for expulsion from the group and social ostracism to do any damage to a system or to attempt to commit fraud for personal profit.

"The biggest crime that has been committed is that of curiosity.... We have been instrumental in closing many security holes in the past, and had hoped to continue to do so in the future. The list of computer security people who count us as allies is long, but must remain anonymous. If any of them choose to identify themselves, we would appreciate the support."

"No member of LOD has ever broken into another system and used any information for personal gain."

And The Plot Thickens

Meanwhile, in Lockport, Illinois, a strange tale was unfolding. The public UNIX system known as *Jolnet* that had been used to transmit the 911 files had also been seized. What's particularly odd here is that, according to the electronic newsletter *Telecom Digest*, the system operator, Rich Andrews, had been cooperating with federal authorities for over a year. Andrews found the files on his system nearly two years ago, forwarded them to AT&T, and was subsequently contacted by the authorities. He cooperated fully. Why, then, was his system seized as well? Andrews claimed it was all part of the investigation, but added, "One way to get [hackers] is by shutting down the sites they use to distribute stuff."

The *Jolnet* raid caused outrage in the bulletin board world, particularly among administrators and users of public UNIX systems.

Cliff Figallo, system administrator for *The Well*, a public UNIX system in California, voiced his concern. "The assumption that federal agents can seize a system owner's equipment as evidence in spite of the owner's lack of proven involvement in the alleged illegal activi-

(continued on page 34)

THE SECRETS

by The "Q"

MIZAR is a Bell system used by the RCMAC (Recent Change Memory Administration Center), also known as the CIC in some areas. Its purpose is to process Recent Change Messages. Before we go into more detail, we will need to familiarize you with some terms.

First off, every Central Office (Wire Center, End Office, whatever) houses one or more switches, whether electromechanical, electronic (analog), or digital. Each switch is responsible for controlling various aspects of telephone service for one or more (usually more) exchanges. Switches in general can be classified into two main types: mechanical and SPCS. Thusly, SCC's (Switching Control Centers) are divided into separate branches. There are the E & M SCC (electromechanical) and the SPC SCC, which handle Stored Program Control Switches. The latter are computer controlled by software, whether they are older versions such as the 1 or 1A ESS (which use crossbars to complete calls) or digital switches such as the 5ESS or DMS100. Henceforth in this article, we will refer to SPCS switches as "electronic" switches, whether analog or digital.

MIZAR is a fortress containing a wealth of resources.

Basically speaking, a switch's memory can be thought of in three main parts: Call Store (CS), Program Store, and Recent Change. In general, a Recent Change Message is a batch of commands which tell the switch to perform an action on a facility (a TN, an OE, TRKGRP, etc.) The Program Store can be thought of as "ROM" memory. This program controls things behind the scenes such as interpreting and processing your commands, etc. Usually at the end of the day, Recent Changes which were processed that day are copied into the Call Store, which is a permanent memory storage area, somewhat "finalizing" the Recent Changes (although they could always be changed again). The 5ESS is similar to this, though it has many operational differences in processing Recent Changes, and Recent Changes are called "SERVORD's" on DMS machines and go into tables when processed.

Now that you are somewhat familiarized with some basic terminology, we will proceed in describing the operation of the MIZAR system. Like we said earlier, MIZAR processes Recent Change Messages (orders), which can be computer generated (by COSMOS, FACS flow-thru, etc.) or manually entered by the CIC. CIMAP (Circuit Installation Maintenance Assist Package) is a sub-system used by both the frame technicians and CIC. "CIMAPs" are primarily generated for new connection (NC) type orders. At the CIC there are three main types of orders processed: changes on a facility, snips, and restorals. Changes could be, for instance, modifications of line attributes. Snips are complete

disconnects (CD's) which must be carried out on a switch in order to complete a CD type order. "Snip" is a term referring to what was done at the frame, i.e. a cable and pair's termination at the CO was "snipped" from the frame, hence a disconnect. "Restoral" is just the opposite of a snip. A cable and pair is being "restored", i.e. reconnected to the frame, and must now be activated at the switch and will hence be in-service once again.

On the average, a single MIZAR system handles Recent Change processing for about 20 switches (and it *can* handle more than that).

Every day, MIZAR logs into COSMOS automatically, usually at the end of the day, to retrieve Recent Change Messages which must be carried out in order to complete a pending service order. COSMOS takes a service order, and based on what is required, is able to generate an RCM from its tables in /usr/rcmap (on PDP-11's) or /cosmos/rcmap (on 3B20S or Amdahl's) which provides COSMOS with information concerning what type of switching equipment is associated with the wire center in effect and uses these tables to create the RCM accordingly. There are four main commands on COSMOS associated with Recent Changes. They are: RCS (to obtain a Recent Change Summary), RCR (to obtain a Recent Change Report), which would allow you to display an RCM if one was associated with a specific service order (all based on the filter options you specify for the search), RED (Recent change EDitor), which allows you to edit a Recent Change Message pending, and lastly, RCP (Recent Change Packager), which generates an RCM for one or more service orders to be processed by MIZAR.

After MIZAR retrieves RCM's from COSMOS, etc. it connects to the desired switch's recent change channel and the message is processed on the switch. MIZAR can connect to switches in various ways, depending upon its configuration. Switches may be accessed on dialup lines, X.25, or by dedicated hardwired connections. Switches can be accessed for the purpose of manually processing service orders with the ONS command. Once on the desired switch, it would be proper to utilize the RCM processing service provided through the MIZAR software, which will cause the service order to be properly logged to MIZAR's switch log (located in /tmp/swXX.out, where XX is the numerical code assigned to that switch), so that all will be up to date and accurate. However, if the RCM is entered straight onto the switch without letting MIZAR's log know, then an "unaccounted for" RC will be processed without ever being logged (except of course on the switch's rollback). COSMOS can be manually accessed with the ONC command. Orders can be queued and have their statuses checked with the ORI/ORS/VFY/etc. commands.

The coupled power of COSMOS and a small army of switches to do your bidding is a treasure worth its weight in gold.

When one first logs into MIZAR it

WHAT MIZAR CAN DO

should be noted that the login would be RCxx or RSxx, where xx represents the account number belonging to that specific RCMAC (CIC). For example, RC01, RS02, etc. Passwords, of course, could be anything within the standard Unix eight character limit. After receiving a login message, you will be prompted with an "SW?" and a "UID?". SW stands for what switch you wish to be logged in as (i.e. once logged in, any transactions would be reflected upon that actual switch). Hitting "?" will provide you with the list of switch identifiers available. They can be two letters (like on COSMOS) or more (which is usually the case, as part of the identifier indicates the type of electronic switch).

The UID must be a valid three letter code which would authorize that particular user to perform transactions with the desired switch. Typical UID's to be aware of are "all" and "any" which usually will work in conjunction with any switch you try to log in under. SW and UID must be provided for the purpose of setting up environment variables used by the MIZAR software. This is done in your .profile.

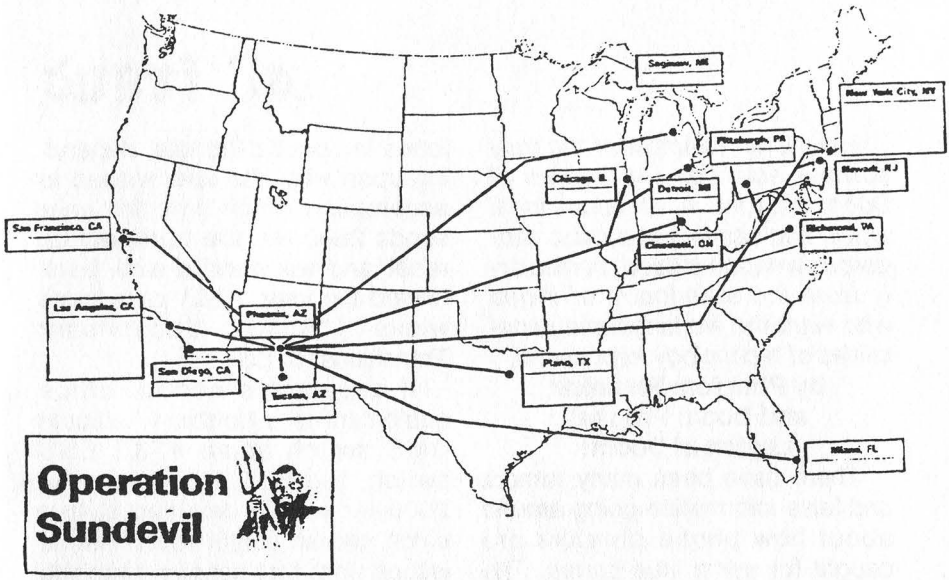
The typical MIZAR user's commands are located in the path /mms/mms (and are all three letters long). It should be noted that CFS on MIZAR is meant to be accurate and up to date with COSMOS'.

Some useful MIZAR commands are: MAR, which lists a MIZAR Activity Report, telling you what MIZAR's up to. MAB, Manually Adjust Blackout periods, is an important command. In some areas, MIZAR classifies switches as being in a "blackout period" at a certain time late in the day (usually the evening), as probably no one would be on that late, or possibly work is being done on the switch. Establishing a blackout period disables normal users from accessing a particular switch from MIZAR. On the other hand, MAB can be used to ENABLE a switch, and remove it from the blackout state. However, the CIC usually closes at 6PM (sometimes staying open as late as 9PM), and logins at such a late time would be foolish as you may jeopardize your future access. SDR, for Switch Data Report, allows you to list out useful information about the switches you specify — for instance, the NPA and exchanges this particular switch handles (including thousands of groups of DID and IBN blocks), its WC name on COSMOS, its configuration as a FACS/SOAC machine, MIZAR's times to call COSMOS, any preset blackout periods, whether AIS or E911 is available to the switch, all valid UID's for login to MIZAR, and usernames and/or passwords for switches that require them (such as the 5ESS or DMS100), as well as other useful information. WCH (Wire center CHange) allows you to change to another wire center (hence, further transactions apply to that wire center).

As you may have noticed from this article, MIZAR is a very useful system indeed. It's a fortress containing a wealth of resources. The coupled power of COSMOS and a small army of switches to do your bidding is a treasure worth its weight in gold.

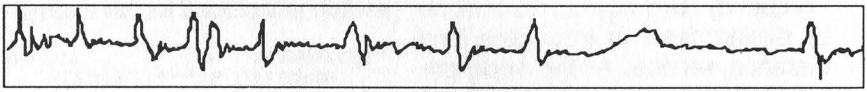
This article was meant to familiarize the reader with the MIZAR management system. We welcome any questions you may have, and we will take pride in providing further articles on similar Bell systems and subjects, so as to better inform the curious mind.

Bart Simpson is one rad dude.

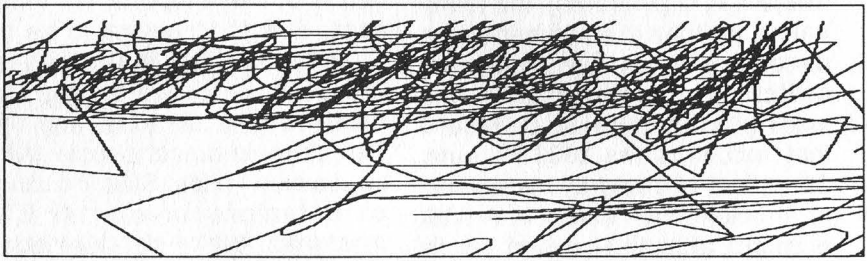


As we went to press, the largest hacker raid in history started happening. There aren't many details we can give you in this issue except to say that this is the first one we know of that had a name. 150 Secret Service agents were involved and tens of thousands of disks have been seized. This is all in addition to the raids spoken of elsewhere in this issue. Look for more details on this in the summer issue. And feel free to send us clippings from your local papers.

These are the brain waves of a normal American teenager.



These are the brain waves of the same teenager after hacking.



When you hack, you're overusing your brain and are liable to find out things you shouldn't.

THE PARTNERSHIP FOR A HACKER-FREE AMERICA

Here is an example of the truly horrible activities the Legion of Doom engaged in. An educational article such as this is a most dangerous weapon indeed, particularly from the standpoint of those who want the workings and capabilities of technology kept secret.

by Phantom Phreaker
and Doom Prophet
Legion of Doom!

There have been many rumors and false information going around about how phone phreaks are caught for using blue boxes. The purpose of this article is to dispel the rumors and myths circulating about this topic.

When a person attempts to access the telephone network with a blue box, they first must have an area that they can use to gain access to an in-band Single Frequency (SF) trunk. This is done by dialing direct or through a long distance service. At the appropriate time, the person sends a 2600 Hz tone through the telephone where it is registered by the terminating switching equipment as a disconnect signal. The terminating switching equipment or trunks leading to this office will be reset if they recognize the 2600 Hz tone. The effect of doing this is a wink, or an interruption in circuit. A wink is heard after the person sends 2600 Hz, and it sounds like a quiet "chirp" or sometimes a "kerchunk". From here, the person can signal to a trunk with Multi-Frequency tones in specific formats, depending upon what the user wished to accomplish. Each time the user sends 2600 Hz, the trunk will be reset and will send a wink back toward the user. AT&T calls these winks "Short Supervisory Transitions" or SST's.

If a person's central office equipment is a Northern Telecom DMS switch or an AT&T ESS switch, the SST caused by the 2600 Hz will be detected at that office and an output report will be issued from that specific switching system. In No. 1 and No. 1A ESS switches, these reports are called SIG IRR reports, or "SIGnal Irregularity" reports. They will be output with the appropriate information relating to the subscriber who initiated the SST. A sample SIGI report from a No. 1A ESS switch is included for an example.

```
* 32 SIG IRR 69      0                00000
    000 555 1111  B8**3*BBBBBBBBB
```

We are unfamiliar with the details of these reports, but in this case, 555 1111 seems to be the Directory Number that originated the SST. Suffice it to say that these reports do exist and that they do help detect people trying to use blue boxes. SIGI is a *standard* feature in all 1A ESS machines. We're not sure about No. 1 ESS, but nearly all the other ESS machines most likely have SIGI or something similar to it.

In the case of NTI's DMS-100

switch, the feature is called "BLUEBOX". The BLUEBOX feature in DMS-100 is not standard. It can be implemented only by telco personnel activating it via a MAP (Maintenance and Analysis Position) channel. The DMS-100 reports are more detailed than the 1A ESS reports, possibly due to the fact that the DMS-100 switch is much newer than the 1A. DMS will recognize the trunk wink and then output a report. The system further checks for the presence of MF tones. If the MF tones are present, and are followed by an ST signal, another report is then generated by the switch. The calling number and called number (in MF) can then be recorded on AMA tape for further investigation by security personnel. In areas with past instances of toll fraud (blue box usage) and in major cities, it can be assumed the BLUEBOX series of features would be implemented. In rural and small town areas, there is less of a chance of this feature being present. The plain fact that this feature exists should be enough to keep you from trying anything foolish.

Since most electronic/digital switching systems have provisions in them to catch blue boxers, one may wonder how to box safely. The safest method of blue boxing would be to not let an SST show up on your line. This can be accomplished by boxing through a long distance service via dialup (Feature Group A or B). The only catch is that the long distance service that you use must not send back a wink when you attempt to box over its network. If an FG-B accessible trunk running from a toll office to an alternate carrier's facilities recognizes your 2600 Hz tone and disconnects, then SIGI or BLUEBOX would indicate your existence and you could be punished for your crime. So, if you must try such things, they are best done from someone else's line or from a coinphone.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

Photo Salvation
Ken Copel

Design
Zelda and the Right Thumb

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Log Lady, The Plague, The Q, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Mr. Upsetter, Violence, and the faithful anonymous bunch.

Remote Observations: Geo. C. Tilyou

BUILDING A DTMF DECODER

by B/Square and Mr. Upsetter

Imagine this scenario: you are listening to your scanner, monitoring a neighbor using his cordless phone. He is accessing his bank-by-phone account. He enters his password, and you hear the whole thing. But the only problem is that he entered the password using touch tones. How do you know which numbers he entered?

Or think of this: you're doing an investigation and recording telephone calls. The person under surveillance is making calls with a touch tone phone and you have tapes of everything. But how do you find out what numbers were dialed?

One answer to these problems would be to buy a commercial DTMF (touch tone) decoder or a similar device called a pen register. These items could cost you a few hundred dollars. The other solution is to build the handy "snatch 'n latch" DTMF decoder presented here for about $35 to $45.

This circuit uses a single chip to decode 12 or all 16 DTMF tones, as selected by the user. Up to 16 tones are stored in the circuit's static RAM memory. Once the tones are in memory, the user reads them out one by one on the circuit's LED display. The circuit can be hooked up to a telephone line, a scanner, or a tape recorder. Now let's take a look at how this little device works.

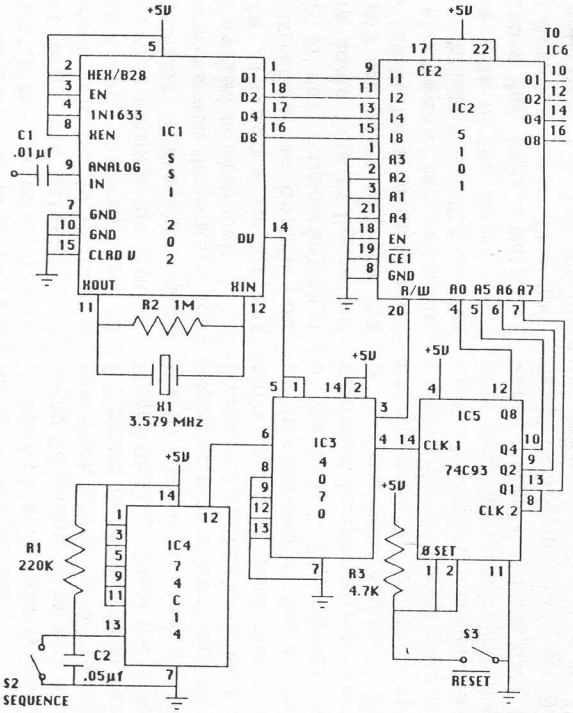
Theory of Operation

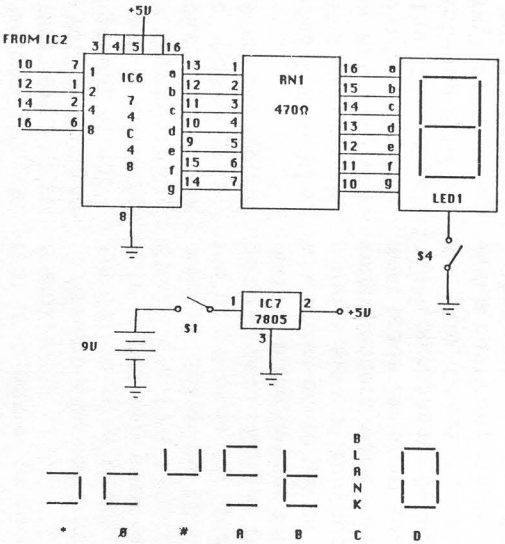
DTMF signals are coupled to pin 9 of IC1, the DTMF decoder chip, by .01 uf capacitor C1. The tones are band split sampled and a coded output is placed on D1, 2, 4, 8, of IC1. Data valid (pin 14) goes high 7 usec. after data is on bus causing the R/W input of the RAM, IC2, to go low and the CLK1 input (pin 14) of the counter, IC5, to go high by way of IC3, the XOR. At this time, the digit received is displayed on LED1 while preconditions (to write the data to memory) are established. 45 msec. after the tone ends, DV goes low, writing the data into RAM and incrementing the counter one count. Code has been written into address 00 of the RAM with the next address presented to A0, 5, 6, 7 of the RAM. 4.56 msec. after DV goes low, the outputs D1, 2, 4, 8 of the decoder clear. This sequence will continue until addresses 00 through 15 contain data. At this time, the counter recycles and data will be written over what was previously stored.

To read out the contents of memory, S3 is opened, causing pins 1 and 2 of the counter to go high. This resets the counter address bus to 00. The data in address 00 of the RAM is presented to IC6, the BCD to 7-segment driver. IC6 converts the RAM output data to a digit which is read out on LED1. When S2 is closed, pin 12 of IC4, the Schmitt trigger, goes high. This causes pin 14 of the counter to go from low to high by way of the XOR. This increments the counter and presents the next address to the RAM, and the next digit is read out. S2 is repeatedly pressed until all the contents of memory have been displayed.

Circuit Construction

There are two different tech-


+5V
HEX/B28
EN
1N1633
XEN
IC1
ANALOG IN
GND
GND
CLKD V
XOUT
XIN
DV
D1
D2
D4
D8
C1
.01µf
R2 1M
X1
3.579 MHz
IC2
CE2
A/W
A0 A5 A6 A7
A3
A2
A1
A4
EN
CE1
GND
TO IC6
IC3
4070
IC5
74C93
CLK 1
CLK 2
Q8
Q4
Q2
Q1
8 SET
R3
4.7K
IC4
7414
R1
220K
C2
.05µf
S2
SEQUENCE
S3
RESET


+5V
FROM IC2
IC6
7448
RN1
470Ω
LED1
S4
9V
S1
IC7
7805
BLANK

niques you can use to construct your own DTMF decoder. These are wire wrap and soldering. In fact, before you decide to build a permanent unit, you may want to put the circuit together on a plastic breadboard. The authors have built units in these three ways and they all worked equally well.

There are some important things to consider before you start. It is very important that you take some time to figure out where you are going to place the IC's to facilitate a "clean" project. This means, for example, that you shouldn't put IC1 on the opposite side of the board from IC2 because they have a data bus running between them. This may get complicated, but it is important to figure out a good parts layout before you start soldering things together. Also, it is a good idea to buy all the parts, including PC board, enclosure, sockets, switches, etc. before you get started on a permanent unit so you can plan how you are going to put everything together. In addition, unless you are a soldering whiz, it is highly recommended that you use sockets for all the IC's. This also makes troubleshooting the device and replacing IC's easier.

This project uses CMOS IC's, which are static sensitive. Theoretically you and your soldering iron should be grounded when handling the IC's. If you don't have an anti-static workstation handy, don't worry about it too much. Try not to touch the pins of the IC's and store them in conductive foam or a piece of tin foil when not in use.

Assembly is readily achieved using 30 gauge hand wire wrap on the back plane of a "universal" PC board (available from Jameco, Radio Shack). Once the layout of the IC's is determined, solder two opposing pins of each socket to the board and methodically wire pin to pin keeping in mind that the pinout is reversed on the wiring side of the board. The crystal can be mounted horizontally or vertically, but the 7805 regulator should be mounted horizontally for low profile. The 30 gauge wire is soldered directly to the switches and jack. Doublechecking your work at various stages will assure a functional device at power-up. Before you insert the IC's into the sockets, check all connections with a continuity meter. Should the circuit not operate, suspect your work before questioning the IC's. The advantage of wire wrap is that it is easier to correct your mistakes.

Assembly by soldering is quite similar to wire wrap. A board with a pattern such as Radio Shack p/n 276-162 is recommended. Solder the IC sockets to the board once you decide on a good layout. Solder the other parts in place. Solder small gauge wires from pin to pin on the component side of the board. Use small jumpers made from component leads for short connections on the component side and the solder side. Check all connections with a continuity meter.

When you put the IC's in their sockets, remember to put them in the correct way, not backwards.

YOUR VERY OWN TOUCH TONE DECODER

As good circuit design practice you may want to put .1 uf capacitors between the power supply pins of each IC and ground. The device will work without them, however.

After you are done with the PCB, think about where you are going to put the LED display, input jack, and switches on your enclosure. Assembly and disassembly will be easier if all of these things are attached to one half of your box.

Using the Decoder

Using the "snatch 'n latch" isn't too hard, but there are a few details about its operation that we need to observe. When you first turn the unit on, be sure to hit the reset switch. This ensures that the tones (or rather the data sent from the decoder to memory) will be stored in the first memory location. Then you sit back and wait for some DTMF tones to come down the line. When they do, the device will snatch 'em and stash 'em in the memory. When the tones have stopped, hit the reset switch. You will see a number on the display, which is the number stored in the first memory location. Hit the sequence button and the numbers in the subsequent memory locations will be read out. Once you've read out all the numbers and written them down somewhere, hit the reset switch again. You are ready to start all over again. The numbers will be in memory as long as the power is on and new numbers haven't been written over the old ones. (That's why you may want to write down the numbers, because any new numbers that come in will erase the old ones.)

There are a few other helpful hints that can make using the decoder easier. First of all, install that switch to turn the LED display on and off. You only need the display when you're reading out numbers, and switching it off will prolong battery life. Also, while reading out the numbers, you might want to remove the device from the phone line or whatever it is hooked up to. If the decoder happens to receive a tone while you're reading out the numbers in memory, the tone will be stored in whatever memory location you happen to be at and generally make things confusing.

One feature of the "snatch 'n latch" that makes it less attractive than commercial models is that it can only store 16 tones. If more than 16 tones are read by the decoder, the counter resets the RAM to the first memory location and the excess tones are read into memory, erasing the previous ones. This is a problem since information is lost. If you anticipate reading in more than 16 tones at one time, you can record the tones on tape and play them back a few at a time into the decoder.

When using the decoder with a tape recorder, hook it up to the earphone jack and adjust the volume so the decoder will read the tones off the tape. The decoder isn't terribly picky about input levels, but theoretically the input level should be less than the supply voltage, which is 5 volts DC. When using the decoder with a scanner, it's best to hook it up to a "tape out" jack if it has one.

BUILDING A DTMF DECODER

Otherwise you can hook it up to the earphone jack. The decoder works like a charm when hooked up directly to a phone line (parallel connected), as the capacitor on the input of the DTMF decoder IC blocks the phone line's DC voltage. However, if you are going to hook up the "snatch 'n latch" to the phone line for any extended period of time, circuitry must be added to the input to protect the device from the ringing voltage. 90 volts AC on the line will surely wreak havoc on the CMOS IC's.

Applications

The DTMF decoder has many interesting uses. Basically, anytime you hear a tone and want to know what it is, hook up the decoder and let it go to work. When it is hooked up to a phone line, the number dialed can be decoded. You can also decode DTMF tones (e.g. passwords) used for services like bank-by-phone, credit card verification, voice mail systems, etc. Calling card numbers can be obtained in the same way if they are entered by touch tone. If you monitor cordless or cellular phones with a scanner, you can hear a lot of this type of DTMF tone use. With a scanner you can also decode such things as access tones for repeaters. DTMF signaling is so widespread there's no doubt that you will discover other useful applications.

The "snatch 'n latch" DTMF decoder presented here is a cost-effective circuit that is an invaluable tool for the telephone experimenter. We hope this article will start you on your way towards building your own.

Parts List

C1- .01 uf
C2- .05 uf
R1- 220K, ohm, 1/4 watt
R2- 1M ohm, 1/4 watt
R3- 4.7K ohm, 1/4 watt
RN1- 470 ohm
X1- 3.579 MHz colorburst, HC-18 case
S1, S4- SPST switch
S2- momentary, normally open
S3- momentary, normally closed
LED1- 7 segment, common cathode
IC1- SSI202, DTMF decoder
IC2- 5101, 256x4 SRAM
IC3- CD4070, quad XOR
IC4- 74C14, hex schmitt trigger
IC5- 74C93, ripple counter
IC6- 74C48, BCD to 7-segment
IC7- 7805, 5V regulator
Misc. parts: 1/8 inch jack, IC sockets, PC board, 9V battery and clip, .1 uf capacitors, enclosure, mounting hardware.

All of the IC's except for IC1 are available from Jameco Electronics, 1355 Shoreway Road, Belmont, CA 94002 (415) 592-8097. They also have sockets, the crystal, and other parts. Some parts are also available from Mouser Electronics. Call 800-992-9943 for a free catalog. The SSI202 DTMF decoder IC is available from W.E.B., PO Box 2771, Spring Valley, CA 92077 for $12.95 plus $2.50 postage and handling.

SILVER BOX BORN IN U.K.

by Tamlyn Gam

There was an article about the construction of a silver box in the Winter 1989/90 issue and it led me to wonder how this would work in the United Kingdom and Europe.

Much of the UK is still using pulse dialing and the use of tone phones is only just spreading. (Most still convert the tone to a pulse for the sake of the antiquated phone system.) As the use of tone systems spreads, now at an increasing pace, there would seem to be a rich area for experiment here. It is not easy to come across a tone phone over here so I had to look for another source for the box parts. The main use here of tones is to control remote devices over telephone lines. These services which are common in the US are only just beginning to come into general use here, but we are now able to use tone controlled answerphones and tone controlled services such as voice banks and bank services. With the lack of tone exchanges and phones, the suppliers of such services have been offering small tone generators to prospective customers (sometimes free). Any hacker worth his salt will have one or three.

I dug out one of mine and pulled it to pieces and, yes, it was run by a 5087 chip. A quick look at the circuit showed it to be the same as the phone described in the earlier article, so I fitted a changeover switch as suggested and am now the proud owner of a silver box.

I am not sure just what I can do with it but time will tell. The received wisdom is that the extra tones are not used in the UK, but I see that the telephone workers are equipped with tone generators having 16 buttons. An "innocent" question as to what all those extra buttons were for has not yet yielded results — but it will. In the meantime I will poke the extra tones about to see what they do and report back. I do work in an office with an internal tone phone service with national links to the public network so I have lots of places to experiment. I will report back here and in the meantime will see what our US colleagues turn up as they blaze the trail.

LISTENING IN

by Mr. Upsetter

Every now and then, those of us who take the time to be observant stumble across something remarkable. Let me relate to you one of those experiences. It was an all too lazy sunny afternoon in Southern California. I was bored, and I decided to listen to my Realistic PRO-2004 scanner. I flipped it on and scanned through the usual federal government, military aviation, and cordless phone frequencies, but there was no good action to be found. I happened across some scrambled DEA transmissions and a droning cordless phone conversation by some neighbors I could not identify. So for a change I scanned

LISTENING TO PHONE CALLS

A reader tells us:

"Be advised that cordless phones are quite easy to monitor, and yours is just as accessible to eavesdropping as anyone's. But there's a hidden danger with some cordless units — they may be transmitting your personal conversations even when not in direct use! This occurs with our newish General Electric System 10, model 2-9675.

"I discovered this "feature" one day when my wife called home while my scanner was whizzing away between 40-50 MHz. I answered on the wired office phone at my desk, with the cordless remote unit hung on the wall on the far side of the kitchen and its base unit cradled in the bedroom. Suddenly, our voices echoed throughout the room! The scanner had hit the 46.xxx MHz frequency the base unit uses to transmit both sides of the conversation and was functioning as a wireless speakerphone!

"I should emphasize that anything you disseminate on any phone circuit may be monitored by someone — the cordless phone just increases the number of possible intercepts, and lowers the level of expertise required to violate your privacy."

through the marine radio channels.

The scanner stopped on marine radio channel 26, which is used for ship-to-shore telephone calls. A man was reading off his calling card number to the operator, who gladly accepted and connected his call. Calling card numbers over the airwaves! I was shocked — astonished that such a lack of security could not only exist, but be accepted practice. I began monitoring marine telephone to find out more, and it turns out that using a calling card for billing is commonplace on VHF marine radiotelephone.

People use calling cards for billing all the time. That's what they are for. But is it that big of a deal? You bet it is. Marine telephone uses two frequencies, one for the ship and one for the shore station. The shore station transmits both sides of the conversation at considerable power, enough to offer reliable communications up to 50 miles offshore. Anyone with a standard police type scanner costing as little as $100 can listen in. People using marine radiotelephone can be broadcasting their calling card number to a potential audience of thousands. And that just shouldn't be happening.

But it is. And there is no doubt that calling card fraud is occurring because of this lack of security. From the phone company's (many Bell and non-Bell companies provide marine telephone service) point of view it must be a trade-off

for customer convenience. You see, there just aren't that many ways to bill a ship-to-shore call. Most calls are collect, a few are billed to the ship if they have an account, and a few go to third party numbers or other special accounts.

Sometimes the operators have trouble verifying billing information. I monitored one man, who after racking up $40 worth of AT&T charges was informed that they couldn't accept his international account number. The operator finally coaxed him into giving an address for billing. Calls are often billed to third party numbers without verification. But calling cards make billing easy for both the customer and the phone company involved.

It would also be tricky for a company to not allow calling card use. Doing so would be an inconvenience to customers and would force them to admit a lack of communications security. Of course people using marine radio should already realize that their conversations aren't private, but announcing the fact wouldn't help the phone company at all. In fact, people may place less calls.

The convenience offered by calling cards makes them an easy target for fraud. They can be used by anyone from any phone and with a variety of different long distance carriers via 10XXX numbers. No red or blue box hardware necessary here, just 14 digits. But of course, the number won't be valid for long after all those strange charges start showing up on someone's bill. It should be noted that when a calling card is used, the number called, time and date of call, and location (and often, the number) from which the call was placed are printed on the bill. A fraudulent user could be caught via that information if they were careless. Also, some long distance companies may contact the owner of the card if they notice an unusually high number of charges on the card.

Long distance companies bear the brunt of the bills caused by calling card fraud. However, if you read the fine print, the cards offered by many companies have a certain minimum amount that the customer must pay, say $25 or $50. (Editor's note: We have yet to hear of a case where a phone company got away with charging a customer when the only thing stolen was a number and not the card itself.)

So what's the moral of the story? Simple. *Be damn careful what you say over any radio,* and that includes cordless and cellular telephones. If you are using a calling card, enter it with touch tones. If you happen to make VHF marine radiotelephone calls, bill collect or charge to your phone number as you would to a third party number — without the last

(continued on page 33)

THINK OF WHAT YOU COULD DO WITH $20,000.

That's the amount of money you'll save if you buy the much heralded E911 documentation from us instead of through Bell South. While they've priced this six page document at $79,449, we'll give it to you for only $59,449!* That's a savings of over 25%.

Imagine the thrill of owning a phrase like: "When an occasional all zero condition is reported, the SSC/MAC should dispatch SSIM/I&M to routine equipment on a 'chronic' troublesweep." (Those words by themselves would easily sell for several hundred dollars.)

You know that offers like this aren't made very often. You also know that this kind of information is a treasure well worth dying for which can't be found in stores anywhere. It's a commonly known fact that understanding how the phone company works is a major step towards World Conquest.

So take that step today. Before your neighbor does....

MAKE CHECKS OUT TO "2600 UNBELIEVABLE OFFER".
(AVOID SENDING CASH THROUGH THE MAIL.) THIS OFFER ENDS JULY 31.

* DOES NOT INCLUDE TAX AND SHIPPING.

```
# bigcheese (internet scanner in Shell)
#
# When run off a Unix with Internet access, this program will scan for ALL
# computer systems tied to the network.  Unixes will be placed in a file
# called .UNIXES
# A complete listing of systems (including both Unixes and non-Unix based
# systems will be found in .all.systems
#
# Please note: This is a *simplified* version written in approximately 1 hour.

if [ -z "$4" ]; then
echo "\nUsage: big.cheese xxx xxx xxx xxx"
exit
else
prefix=$1;addr1=$2;addr2=$3;addr3=$4
fi
export prefix addr1 addr2 addr3
while :
do
if [ -f /tmp/stop.scn ]; then
break
fi
echo "\n\r\n\r\n" | telnet "$(prefix).$(addr1).$(addr2).$(addr3)" >/tmp/.chkit&
sleep 10
kill 0
cat /tmp/.chkit >> .all.systems
x=`grep "login:" /tmp/.chkit`
        if [ "$x" ]; then
        echo "`date` => $(prefix).$(addr1).$(addr2).$(addr3)" >> .UNIXES
        fi
if [ $addr3 -gt 255 ]; then
        addr2=`expr $addr2 + 1`;addr3=0
                if [ $addr2 -gt 255 ]; then
                addr1=`expr $addr1 + 1`;addr2=0
                                if [ $addr1 -gt 255 ]; then
                                DONE=1
                                fi
                fi
fi
done
```

WE GET THE MOST INTERESTING FAXES FOR MILES AROUND. SEND YOURS TO 516-751-2608 ANYTIME.

news update

Morris Sentenced

On May 4, Robert Morris, whose runaway worm created havoc on the Internet over the fall of 1988, was sentenced to three years' probation, a $10,000 fine, and 400 hours of community service. He could have received up to five years in prison along with a $250,000 fine.

While it seems pretty strange to sentence somebody for what was, in effect, a scientific experiment gone awry, it certainly is a relief that cooler heads seemed to prevail in this important case. After all, Morris could have wound up in prison. We can only hope this isn't the exception to the rule, or worse, a case of special treatment because his father works for the NSA.

Albania Callable

For many years, the strange and mysterious European country of Albania was completely unreachable by telephone, at least from the United States. But all of that suddenly changed on May 1, when AT&T started providing operator assisted calls there. It's rumored that direct dial service will start in the fall. If so, the country code is 355. The call shown below was made from Canada. Now there are only three countries that are unreachable from the United States: Vietnam, Cambodia, and North Korea. (Actually, it IS possible to call those places from here - can you figure out how?)

No.	Date	Called from	Called to	Time	Rate	Min.	Amount
Calling number 751-2600							
1	FEB 09	SOO ON 705 759-8000	ALBANIASPR	10 AM	PS PERSON	10	$28.60

MCI Insecurity

In an internal memo leaked to 2600, MCI admits that there is very little security for their international calling cards. The "international number" is defined as a 17 to 19 digit number composed of the Telecommunications Industry Identifier (89), the country code (from one to three digits), an MCI issuer identifier (222 or 950), the subscriber number (the same as the first ten digits of the MCI 14 digit domestic number), and a check digit. The international number is used when going through operators overseas, not when using MCI Call USA, the MCI equivalent of

- MCI CONFIDENTIAL -

DO NOT SHOW CUSTOMERS

AT&T's USA Direct.

In a section on fraud, MCI states, "Because there will be no automated validation of the International Number, fraud is a potential issue. However, it should be noted that AT&T has operated this service for over 20 years without validation of its international number." That should paint a pretty clear picture of the effective and immediate solutions some companies come up with when faced with potential security problems.

New York Tel Rate Increase

New York Telephone is asking for some of the most outrageous rate increases in its history. Apart from lowering the nighttime discount rate to 50 percent (from 60 percent) and the evening rate to 25 from 35, the company plans to double the charges for most classes of message-rate service. For instance, if you pay $8 a month for a certain type of service, you can look forward to paying $16 or more in the future. Not only that but charges to local directory assistance from payphones (currently free) will be initiated at a cost of 50 cents per request. The two free requests every customer gets each month will be eliminated. And an unprecedented 50 cent charge will apply to all calls to the operator that don't wind up in a call being processed! The Public Service Commission can deny the rate increase, but if they don't, these outrageous rates will go into effect next January.

Furthermore...

US Sprint has redesigned their bills. And, if you have a 950 access code, you'll be delighted to know that they print your code on every page!

you've found the official

Clarifying REMOBS

Dear 2600:

In reference to your REMOBS article by The Infidel in the Autumn 1989 issue, the author distorted the true definition of Remote Observation in the digital age.

The REMOBS is a hardware device manufactured by TelTone and numerous other electronics manufacturers. To say that it is a Bell standard piece of equipment could not be further from the truth. A typical REMOBS ranges in cost from $800 to $1200 and is always attached to the cable and pair in question at the frame (in the central office). The fact remains that the REMOBS is not totally silent. It is a mechanical device that uses cross-connect circuits to tap into a line, which obviously results in clicks and noises. Unlike The Infidel's notion that a REMOBS can monitor any line in an exchange, it is limited to a minimal number of subscriber lines and is restricted to guidelines set forth by the FCC. Ma Bell uses a series of circuits known as "no test trunks" to monitor lines for testing, and linemen in particular use software driven monitoring devices (TV on LMOS). Whether or not the observer will be heard depends upon the software selection.

To say you don't actually "connect" to a customer's line and simply monitor it is totally wrong. It is impossible to listen in on a conversation if there is no physical connection to the remote line you wish to observe (with the exception of cellular and cordless, etc.).

MOD!
Masters of Deception
New York City

And don't forget satellites and microwave links. It's quite a bit harder to zero in on a particular conversation but there's also a lot more to choose from with virtually no chance of being caught. In addition, DMS-100 switches seem to be gaining a reputation for inadvertently allowing access to other conversations. The story is always the same: you're having a conversation and all of a sudden you're connected to another conversation. You can hear them but they can't hear you. They hang up and you get another conversation. And so on. If there are "clicks" in these instances, nobody seems to be hearing them. Which brings us to an interesting point. If there are telltale sounds involved, how many of us know what they mean? Is every click on our lines someone eavesdropping? Of course not. Are monitoring devices becoming more sophisticated and less "noisy"? Absolutely. These facts, coupled with the increasing number of ways to listen, assures us of the fact that no phone conversation can be considered secure.

Who's Listening?

Dear 2600:

I am the victim of an "Information Source" that has me puzzled. My phones (according to Ma Bell) were not bugged and I know for a fact that no bugs were planted in my office. There was no illegal tap on my phone that I

could detect.

Someone mentioned a new tap that is put into effect by just dialing my number. There is no ring and the listener can hear all that goes on in the room where the phone is. There is also no record of the phone call. This sounds like a combination black box and some other device.

Can you clue me in?

WH
Upstate New York

A harmonica bug, also known as an infinity transmitter, is usually placed in the earpiece of the phone. A particular frequency sent over the phone triggers them to start transmitting. If this was the case here, you should have been able to find it, although some have been made to look like phone jacks. Keep in mind that this is not a tap, but a bug. In other words, it works even when the phone isn't in use, monitoring the room, not the phone line. We're unaware of any "service" that allows someone to call in and do this without first having physical access to the phone. There are maintenance functions within the telephone company that allow lines to be monitored without having to install equipment, but these aren't supposed to be used outside the company. Somehow that doesn't sound very reassuring, does it?

Blue Box Chip

Dear 2600:

Although we are in the twilight of the blue box era, I'm sure many readers would be interested in an excellent blue box IC. The chip is the Teltone M-993 Multifrequency Tone Generator. It generates all 12 MF tones using a standard 3.58 Mhz colorburst crystal.

This chip offers several advantages to blue box designers. All blue box tones are generated accurately by one IC (except for 2600 Hz) and no adjustment or tuning is required. It does have one disadvantage, however. The IC has a 4 bit binary input for tone selection, meaning it isn't easily interfaced with a keypad.

The IC is also expensive, costing anywhere from $14 to $25 for single pieces. I have found two sources: High Technology Semiconductors in California (714) 259-7733 and Almo Electronics with outlets coast to coast (800) 525-6666. Other Teltone distributors sell it too. Teltone Corp. can be reached at (206) 827-9626.

Some distributors will give electronics companies free samples and spec sheets.

Mr. Upsetter

Bugs Wanted

Dear 2600:

If, as The Dark Overlord says, there are many weaknesses in UNIX, why don't you print a few? I frequently see messages on Arpanet saying things like "Major security bug found in XWindows, service representative will contact your site with details, disable XWindows until then" (no, this is not a real message), and there are evidently lots of administrators who know lots of easy-to-exploit bugs/holes in various op systems. Why don't you publish them? To

my knowledge 2600 has *never* published any specific security holes — not even the rhosts bug that the Worm exploited, which everybody except me seems to know about. For instance, Bill Landreth said he broke into a VAX running VMS using a rapid-fire command replacement: a program in C which submitted a command, waited until it was approved, and then wrote a different command into the VMS buffers before it was executed. Someone must have details: formats, specific memory locations, and timing — maybe a similar program.

I know people who have a .COM file on VMS which allows them to send mail messages with bogus "From:" fields. They are unwilling to supply me with it for fear of losing their jobs. Can someone provide a listing? How about ways of faking Arpanet mailer headings? (A practice very common on April 1)

I was recently on a VAX running VMS on which I had read privs for AUTHORIZE.EXE. I copied it into my directory, created a fake template of users, passwords, and privileges, and tried to redefine the appropriate logicals so that I could then SET HOST and login using my fake AUTHORIZE.DAT and get a bogus account pointed at a real directory with real privs. I had no success. Can anyone with access to VMS manuals tell if this is possible, and if so, what logicals to redefine?

Charlie Brown

Questions and Info

Dear 2600:

I have a *lot* to get off of my mind after reading your Winter 89-90 issue. I haven't had a computer for months now so I've been out of the phreak/hack scene for quite a while.

1. What are some of the ways that blue and red boxes can be used and detected on DMS-200 and other new switching systems?

2. When scanning (war-dialing), how many numbers per minute does it take to trip a warning flag at the CO?

3. Are test numbers called from a different area code billed?

4. Are there any other hack/phreak publications past or present?

5. Does anyone have, or has there been printed, a listing of Telenet Network User Addresses (NUA)?

6. What is the Summercon, as listed in the winter issue's Marketplace?

7. I have recently gotten my hands on an M-242A REMOBS unit. I have no idea what it does or how to work it. Any info will be appreciated.

Last of all, here are some interesting numbers in the 704 area code: ANI: 311, ringback: 340-xxxx. Here are some rather different COCOT numbers: 704-334-1051, 704-334-0745. These payphones,

2600 LETTERS, PO BOX 99, MIDDLE ISLAND, NY 11953

of the nineties

if not picked up within approximately 8 rings, will answer with a computer connect tone, followed in about 5 seconds by a very strange tone.

GB

First off, a DMS-200 is a toll switch, meaning it's used only for long distance switching and not in central offices. The #4 ESS is another example of this. Check elsewhere in this issue for details on how blue boxers are detected.

In some places, scanning has been made illegal. It would be hard, though, for someone to file a complaint against you for scanning since the whole purpose is to call every number once and only once. It's not likely to be thought of as harassment by anyone who gets a single phone call from a scanning computer. Some central offices have been known to react strangely when people start scanning. Sometimes you're unable to get a dialtone for hours after you start scanning. But there is no uniform policy. The best thing to do is to first find out if you've got some crazy law saying you can't do it. If, as is likely, there is no such law, the only way to find out what happens is to give it a try.

Test numbers will almost always bill when called from outside the area they're meant for. Sometimes they even bill locally!

We know of no other publication in this country that does exactly what we do, but there are some that have some similarities. When we find out about them and get ahold of a copy, we generally spread the word.

Getting a listing of Telenet addresses is like getting a telephone book. It would be outdated the moment you set eyes upon it. But there are many partial listings floating around, and if we get one in the future we'll share it as we've done in the past.

Re: Summercon, it's an annual gathering of American hackers and phreaks. The details will be announced when we have them.

Finally, the REMOBS unit you have will only work from WITHIN the central office. Those units are used for monitoring trunks, not individual lines, and they're really rather outdated. Still, it can't hurt to have one lying around the house....

Yet Another Threat

Dear 2600:

I think you might find this interesting. It was extracted from the RISKS Digest on USENET.

"The Prodigy Services publication, *Prodigy Star* (Volume III, No. 1) recently showcased a 'major benefit'. The Prodigy system accesses remote subscribers' disks to check the Prodigy software version used, and when necessary, downloads the latest programs. This process is automatic when subscribers link to the network.

"I asked Prodigy how they protect against the possibility of altering subscribers' non-Prodigy programs, or reading their personal data. Prodigy's less-than-reassuring response was essentially (1) we don't look at other programs, and (2) you can boot from a floppy disk. According to Prodigy, the fea-

ture cannot be disabled."

I think it is obvious how to make use of this "feature" for other purposes. Let us hope that this "feature" is removed from one of the newly downloaded versions....

fin

Red Box Woes

Dear 2600:

Since the foneco strike in New York, the outdoor payphones that were vandalized and are now repaired *do not* allow red box usage. Even after putting in the first coin, using the box results in a recorded request to deposit the balance due. They must have done something with the coin detect relay setup. Indoor phones in building lobbies and stores still seem to work okay.

Curious

Throughout most of New York, a new relay system known as MARS has been installed over the last year. You may have noticed a difference in the way the dial tone appears. Some phones may not have been switched over yet. We're looking for more information on this, as well as ways of bypassing the disadvantages.

Dear 2600:

Your latest issue on building a silver box using a Radio Shack dialer was quite good. I would like to know if a modification can be made with a pocket Radio Shack dialer to build a red box.

Please reply by letter since I'm not sure if my subscription is expired.

Rhode Island

There wouldn't be much point to making a red box out of a Radio Shack dialer since a red box only makes a single combination of tones (1700 hz and 2200 hz). One 60 millisecond pulse indicates a nickel, two 60 millisecond pulses indicate a dime, and five 35 millisecond pulses separated by 35 milliseconds indicate a quarter. These tones are not found on a touch tone pad, whereas the silver box tones are. Our Summer 1988 edition has red box plans for those who are interested. It should be noted, though, that many red boxes are nothing more than tape recorders with the appropriate tones cued up.

There's no way we can reply individually to all of the questions we get. It's up to you to keep track of when your subscription is nearing an end. That information should be on your mailing label.

While we're on the subject, folks, a couple of words of advice. When you move, let us know BEFORE your old address becomes invalid. The post office does not forward magazines. Instead, they send us notification of your new address, a service they charge us for. And you wind up missing an issue for no good reason. Also, those of you using aliases: make sure you're able to get mail under that name. There is nothing more frustrating than trying to contact someone whose issues keep coming back to us, especially when they're complaining to us about not getting what they paid for! If you have to use a fake name or handle, just make sure the post office knows about it

so we can all get on with our lives.

Suggestions and Questions

Dear 2600:

Glad to see your you covering phones again. Very much enjoyed the fortress phone article and had a few questions about it.

Green box tones: when are these tones to be sent? When you are still talking? After you hang up and pick up the phone again?

Red box or green box tones: do they have to be sine wave tones or will square wave tones work?

Just what are toll free 950 calls?

What is beige boxing and how is it useful? How about an article for remedials like me?

Redneck 1
San Luis Obispo, CA

Green box tones are simply MF tones used in a different way. For instance, KP is the signal to spit out the change. The MF number 2 is the signal to collect the coins. There are other tones for obscure functions which nobody really uses these days. Keep in mind that these tones are only used on analog switches. The tones must be sent from the called party. The person you call blasts KP, you hang up, and your change should come back, provided it hasn't already dropped.

Either sine wave or square wave tones work just fine.

950's are toll free numbers that provide you with access to the dial tones of other long distance companies. It's necessary to enter an authorization code before or after entering the number you want to call. These dial tones only accept touch tones, not pulse. 950-1022 belongs to MCI, 950-1033 belongs to Sprint, and there are many others floating around just waiting to be discovered.

Beige boxing is nothing more than using someone else's phone line to make a call. This is done quite a bit in dormitories, where it's fairly easy to get access to the phone closet and do some rewiring.

Dear 2600:

Keep up the good work. I like a balance between telephony and computers: software and hardware. The international info is valuable. You ought to combine this and one of the other magazines into a real, full-blown rag like Data Communications. How about a feature on the ATT System 75/85 PBX?

Satisfied Customer

We'll look into that PBX and see if there's anything particularly interesting about it. At the moment, we have little interest in looking or reading like Data Communications.

Dear 2600:

I have asked you before, but has any new information come up on publications similar to yours in the United Kingdom or the Netherlands? I admire your persistence and philosophy, and hope that you will continue for as long as you feel moved to do so.

An Overseas Fan

There has been talk of a publication starting in England for some time. We'll let you know if any-

thing develops. In the Netherlands, there's Hack-Tic at PO Box 22953, 1100 DL Amsterdam.

Dear 2600:

Would you be interested in an article about computer viruses? I have an Apple, so everything concerning it would be based on Apple assembly language. The article would cover how to make, destroy, and detect viruses on the Apple, and in general. I might supply a simple source code for a non-destructive self-replicating program, if you are interested.

Somewhere in the Midwest

We're surprised you had to ask. We're waiting by the mailbox.

Hotel Phones

Dear 2600:

I recently came across a very major security problem when using private phone systems such as in hotels.

Most of these have a Station Message Detail Recorder (SMDR) which keeps track of all digits entered at your extension. At checkout time these numbers are compared, either electronically or by hand, with a rate chart and the bill gets calculated.

Since I generally use alternative common carriers for long distance calls, I almost always have a local, free (950) access number.

Recently, one institution tried charging me excessive amounts, claiming that I had accessed some of the other, ahem, special exchanges (anything above zero is wrong, but I'll grant them the 25 cents if they insist) so I asked to see the printout.

I discovered, to my very major dismay, that the paper had the 950 calling number *and* my security code, as well as the final number dialed.

On checking further, I discovered this is not only a common feature of SMDR's, but is also on many private coin phones.

Very curious, and very worrisome.

I found a way to (sometimes) get around this. Most of the listings are limited to 20 or so characters, so I will punch in some random characters, and hit the octothorpe for a new dialtone. That way, the hotel printout merely gets the first, defective, series.

This problem certainly raises some curious questions....

DB

New York City

Why do you think so many phone phreaks work in hotels?

The Facts on 10698

Dear 2600:

On pages 42 and 43 of your wonderful Autumn 1989 issue is a comprehensive list of carrier access codes, and in the third column on page 43 is a footnote, the fourth and fifth sentences of which read as follows: "10698, for example, is used to route local calls via New York Telephone. But since all local calls are routed through New York Telephone anyway, it doesn't really serve much purpose except to occasionally get around PBX restrictions."

The second sentence of the

quoted portion above is simply wide of the mark, because you are supposed to use 10698 if you want to route certain interstate inter-LATA calls via New York Telephone instead of via AT&T or another long distance carrier. All local calls — in fact, *all* calls, including local, toll, and long distance calls, which both originate *and* terminate *within* a LATA ("Local Access and Transport Area") — *must* be carried by the local Bell Operating Company (BOC), in accordance with Judge Greene's decree in the antitrust case which resulted in the breakup of the Bell System. Those kinds of calls are often referred to as "intra-LATA calls". Conversely, all calls which originate in one LATA and terminate in another LATA ("inter-LATA calls") *must*, unless the decree carves out an exception, be carried by AT&T or an alternate long distance carrier. As Judge Greene put it in his opinion deciding many of the LATA questions: "Most simply, a LATA marks the boundaries beyond which a Bell Operating Company may not carry telephone calls." That's why the geographic delineation of the LATAs was so important to the BOCs. (Judge Greene's opinion deciding many of the LATA questions may be found beginning at page 990 of volume 569 of "Federal Supplement", which is a series of reports of decisions in the lower Federal courts.)

There are two exceptions to the general inter-LATA call rule which Judge Greene recognized and incorporated into the modified final judgement (the MFJ). Both of the exceptions are in or close to our own backyard (speaking as a resident of Manhattan). Both of the approved modifications recognize and continue a practice which is decades old, and is referred to by Judge Greene in his opinion deciding the question as the "limited corridor exception".

One of the limited corridor exceptions is between five northern counties in New Jersey (Bergen, Essex, Hudson, Passaic, and Union Counties) and New York City (the five boroughs of Manhattan, Bronx, Brooklyn, Queens, and Staten Island). Before the breakup, the New York State portion of the corridor consisted of all the territory in Numbering Plan Areas ("NPAs") 212, 516, and 914, but in his decision, Judge Greene cut the territory down to New York City only (which at that time was NPA 212, but now consists of NPAs 212 and 718). In Judge Greene's words, "The exception would allow New York Telephone and New Jersey Bell to continue their direct switching of traffic and private line demand between New York and New Jersey via Class Five, local trunks, a current 'privileged business' arrangement which would be scaled down from 516 and 914 to New York City only." (Judge Greene's opinion explaining why he decided to make a modification of the final judgement as to the northern corridor appears at page 1018 of volume 569 of "Federal Supplement".)

The other corridor exception is between Philadelphia and its suburbs in Pennsylvania, and Camden

and its suburbs in New Jersey. In Pennsylvania, the territory comprises five counties: Bucks, Chester, Delaware, Montgomery, and Philadelphia. In New Jersey, there are three counties: Burlington, Camden, and Gloucester. (Judge Greene's opinion explaining why he decided to make another modification of the final judgement as to the southern corridor appears at pages 1019 and 1021-1023 of volume 569 of "Federal Supplement".)

I suppose that in the early days when calls were handled by live operators, the high volume of calls in the two corridors prompted New Jersey Bell to find ways to speed up the calling process by bypassing AT&T Long Lines, and New York Telephone, in the northern corridor, and Bell of Pennsylvania, in the southern corridor, were willing to oblige. (One of your readers who is a real old-timer may be able to give us the correct explanation.) At any rate, this venerable practice has persisted, and was incorporated into the MFJ by Judge Greene.

As a consequence, now if you want to make a northern corridor call from an equal access central office in New Jersey to New York City and bypass AT&T (or whatever long distance company has been chosen), you can do so by first dialing "ten NJB" (10652) and then dialing 1-212 plus the Manhattan or Bronx phone number or 1-718 plus the Brooklyn, Queens, or Staten Island number.

In New York City, if you want to bypass the long distance company and use New York Telephone, you must first dial "ten NYT" (10698) to have the call be listed on the New York Telephone section of your phone bill. New York Telephone hints at how to do this in the white pages, but, surprisingly, doesn't give the 10698 access code.

In Pennsylvania, you must dial "ten BPA" (10272) to make a "Jersey Link" call via Bell of Pennsylvania. To make a "Pennsy-Link" call from New Jersey, you would precede the call with "ten NJB" (10652).

So, the codes 10272, 10652, and 10698 are legitimate access codes, but only for a limited purpose: to make corridor calls via a BOC instead of via a long distance carrier.

The County Man

More Network 2000 Ripoffs

Dear 2600:

I, too, had a similar experience with Network 2000 and the Sprint card last summer in a mall in Nashua, New Hampshire (Winter 89-90, Letters).

The advertising at the Sprint booth mentioned only the FON card, and said nothing about changing long distance carriers. When I asked the woman about getting the FON card, she gave me an application to fill out. But before I signed it, I noticed in the fine print that I was agreeing to change my long distance carrier to Sprint.

I asked the woman if I had read the application right. She at first said no, I was applying for the

and information

FON card only. When pressed, however, she finally admitted it, saying, "Well, wouldn't you rather have Sprint?" Only when I declined did she turn the form over, where there was another application for the FON card only.

Needless to say, you know which form was face up on the table, and which form you were told to fill out when you asked for the FON card. It's impossible to tell who the perpetrators were: Network 2000 or their reps.

On another note, ANI in Nashua, NH (and maybe all of 603) was 1-200-222-1111 as of last summer (or maybe it was just 200-222-1111). Oddly enough, it was given to me freely over the phone by a NYNEX tech weenie.

The Iron Warrior
No Fixed Address

Sensitive Material

Dear 2600:

It took close to six weeks to receive my last order of back issues. Do you think customs was pulling some stunts because when I received the parcel it was in a plastic bag and the top of the envelope was ripped and sealed with scotch tape. Is this how you sent them out?

A Dedicated Subscriber

It may take a few weeks to get back issues, but they shouldn't be in a plastic bag or opened in any way. It could have been customs, the post office, or some crazed individual that attacked it somewhere along the line.

Readers: if anything is wrong with your issues, tell us. If there are blank or smudged pages, it's entirely our fault. If your issues are mangled or ripped, it's probably the post office. In that case, tell us AND file a complaint with them.

LISTENING IN *(continued from page 21)*

four calling card digits. For the most part radio communications are easy to intercept, and keeping them secure is up to you.

For those of you with scanners who would like to check out marine telephone, here are the frequencies allocated by the FCC. Monitoring marine telephone is a good way to get an inside look at telephone company operations. If you live near the east or west coast, the Mississippi River or the Great Lakes, there will be marine radio activity. During daylight hours you may hear transmissions from hundreds of miles away due to tropospheric ducting propagation.

VHF Marine Radiotelephone Frequencies

Channel	Ship	Shore
24	157.200	161.800
84	157.225	161.825
25	157.250	161.850
85*	157.275	161.875
26	157.300	161.900
86	157.325	161.925
27	157.350	161.950
87	157.375	161.975
28	157.400	162.000
88*	157.425	162.025

* These frequencies are allocated for uses other than marine radiotelephone in certain areas.

(continued from page 7)

ties (and regardless of the possibility that the system is part of the owner's livelihood) is scary to me and should be to anyone responsible for running a system such as this."

Here is a sampling of some of the comments seen around the country after the Jolnet seizure:

➔ "As administrator for *Zygot*, should I start reading my users' mail to make sure they aren't saying anything naughty? Should I snoop through all the files to make sure everyone is being good? This whole affair is rather chilling."

➔ "From what I have noted with respect to *Jolnet*, there was a serious crime committed there — by the [federal authorities]. If they busted a system with email on it, the Electronic Communication Privacy Act comes into play. Everyone who had email dated less than 180 days old on the system is entitled to sue each of the people involved in the seizure for at least $1,000 plus legal fees and court costs. Unless, of course, the [authorities] did it by the book, and got warrants to interfere with the email of all who had accounts on the systems. If they did, there are strict limits on how long they have to inform the users."

➔ "Intimidation, threats, disruption of work and school, 'hit lists', and serious legal charges are *all* part of the tactics being used in this 'witch-hunt'. That ought to indicate that perhaps the use of pseudonyms wasn't such a bad idea after all."

➔ "There are civil rights and civil liberties issues here that have yet to be addressed. And they probably won't even be raised so long as everyone acts on the assumption that all hackers are criminals and vandals and need to be squashed, at whatever cost....

"I am disturbed, on principle, at the conduct of at least some of the federal investigations now going on. I know several people who've taken their systems out of public access just because they can't risk the seizure of their equipment (as evidence or for any other reason). If you're a Usenet site, you may receive megabytes of new data every day, but you have no common carrier protection in the event that someone puts illegal information onto the Net and thence into your system."

"The biggest crime that has been committed is that of curiosity."

Increased Restrictions

But despite the outpourings of concern for what had happened, many system administrators and bulletin board operators felt compelled to tighten the control of their systems and to make free speech a little more difficult, for their own protection.

Bill Kuykendall, system administrator for *The Point*, a public UNIX system in Chicago, made the following announcement to the users of his system:

"Today, there is no law or precedent which affords me... the same legal rights that other common carriers have against prosecution should some other party (you) use my property (*The Point*) for illegal activities. That worries me....

"I fully intend to explore the legal questions raised here. In my opinion, the rights to free assembly and free speech would be threatened if the owners of public meeting places were charged with the responsibility of policing all conversations held in the hallways and lavatories of their facilities for references to illegal activities.

"Under such laws, all privately owned meeting places would be forced out of existence, and the right to meet and speak

AND INTRUSIONS

freely would vanish with them. The common sense of this reasoning has not yet been applied to electronic meeting places by the legislature. This issue must be forced, or electronic bulletin boards will cease to exist.

"In the meantime, I intend to continue to operate *The Point* with as little risk to myself as possible. Therefore, I am implementing a few new policies:

"No user will be allowed to post any message, public or private, until his name and address has been adequately verified. Most users in the metropolitan Chicago area have already been validated through the telephone number directory service provided by Illinois Bell. Those of you who received validation notices stating that your information had not been checked due to a lack of time on my part will now have to wait until I get time before being allowed to post.

"Out of state addresses cannot be validated in the manner above.... The short term solution for users outside the Chicago area is to find a system closer to home than *The Point*.

"Some of the planned enhancements to *The Point* are simply not going to happen until the legal issues are resolved. There will be no shell access and no file upload/download facility for now.

"My apologies to all who feel inconvenienced by these policies, but under the circumstances, I think your complaints would be most effective if made to your state and federal legislators. Please do so!"

These restrictions were echoed on other large systems, while a number of smaller hacker bulletin boards disappeared altogether. We've been told by some in the hacker world that this is only a phase, that the hacker boards will be back and that users will once again be able to speak without having their words and identities "registered". But there's also a nagging suspicion, the feeling that something is very different now. A publication has been shut down. Hundreds, if not thousands, of names have been seized from mailing lists and will, no doubt, be investigated. The facts in the 911 story have been twisted and misrepresented beyond recognition, thanks to ignorance and sensationalism. People and organizations that have had contact with any of the suspects are open to investigation themselves. And, around the country, computer operators and users are becoming more paranoid and less willing to allow free speech. In the face of all of this, the belief that democracy will triumph in the end seems hopelessly naive. Yet, it's something we dare not stop believing in. Mere faith in the system, however, is not enough.

We hope that someday we'll be able to laugh at the absurdities of today. But, for now, let's concentrate on the facts and make sure they stay in the forefront.

➔ Were there break-ins involving the E911 system? If so, the entire story must be revealed. How did the hackers get in? What did they have access to? What could they have done? What did they actually do? Any security holes that were revealed should already have been closed. If there are more, why do they still exist? Could the original holes have been closed earlier and, if so, why weren't they? Any hacker who caused damage to the system should be held accountable. Period. Almost every hacker around seems to agree with this. So what is the problem? The glaring fact that

"The facts in the 911 story have been twisted and misrepresented beyond recognition, thanks to ignorance and sensationalism."

WELCOME TO THE 90'S

there doesn't appear to have been *any* actual damage. Just the usual assortment of gaping security holes that never seem to get fixed. Shoddiness in design is something that shouldn't be overlooked in a

"Putting the blame on the hackers for finding the flaws is another way of saying the flaws should remain undetected."

system as important as E911. Yet that aspect of the case is being side-stepped. Putting the blame on the hackers for finding the flaws is another way of saying the flaws should remain undetected.

→ Under no circumstance should the *Phrack* newsletter or any of its editors be held as criminals for printing material leaked to them. Every publication of any value has had documents given to them that were not originally intended for public consumption. That's how news stories are made. Shutting down *Phrack* sends a very ominous message to publishers and editors across the nation.

→ Finally, the privacy of computer users must be respected by the government. It's ironic that hackers are portrayed as the ones who break into systems, read private mail, and screw up innocent people. Yet it's the federal authorities who seem to have carte blanche in that department. Just what did the Secret Service do on these computer systems? What did they gain access to? Whose mail did they read? And what allowed them to do this?

Take Exception

It's very easy to throw up your hands and say it's all too much. But the facts indicate to us that we've come face to face with a very critical moment in history. What comes out of this could be a trend-setting precedent, not only for computer users, but for the free press and every citizen of the United States. Complacency at this stage will be most detrimental.

We also realize that one of the quickest ways of losing credibility is to be shrill and conspiracy-minded. We hope we're not coming across in this way because we truly believe there is a significant threat here. If *Phrack* is successfully shut down and its editors sent to prison for writing an article, *2600* could easily be next. And so could scores of other publications whose existence ruffles some feathers. We *cannot* allow this to happen.

In the past, we've called for people to spread the word on various issues. More times than not, the results have been felt. Never has it been more important than now. To be silent at this stage is to accept a very grim and dark future.

(clip and save)

WHAT MAKES IT ALL WORTHWHILE (COMPLETE AND UNABRIDGED)

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

the scoop on 911

Documentation on the E911 System
March 1988
$79,449, 6 pages
Bell South Standard Practice
660-225-104SV

Review by Emmanuel Goldstein

It otherwise would have been a quickly forgotten text published in a hacker newsletter. But due to all of the commotion, the Bell South E911 document is now very much in the public eye. Copies are *extremely* easy to come by, despite Bell South's assertion that the whole thing is worth $79,449.

While we can't publish the actual document, we can report on its contents since it's become a news story in itself. But don't get excited. There really isn't all that much here.

Certain acronyms are introduced, among them Public Safety Answering Point (PSAP), also known as Emergency Service Bureau (ESB). This is what you get (in telco lingo) when you dial 911. The importance of close coordination between these agencies is stressed. Selective routing allows the 911 call to be routed to the proper PSAP. The 1A ESS is used as the tandem office for this routing. Certain services made available with E911 include Forced Disconnect, Alternative Routing, Selective Routing, Selective Transfer, Default Routing, Night Service, Automatic Number Identification, and Automatic Location Identification.

We learn of the existence of the E911 Implementation Team, the brave men and women from Network Marketing who help with configuration in the difficult cutover period. This team is in charge of forming an ongoing maintenance subcommittee. We wouldn't want that juicy tidbit to get out, now would we?

We learn that the Switching Control Center (SCC) "is responsible for E911/1AESS translations in tandem central offices". We're not exactly shocked by this revelation.

We also find out what is considered a "priority one" trouble report. Any link down to the PSAP fits this definition. We also learn that when ANI fails, the screens will display all zeroes.

We could go on but we really don't want to bore you. None of this information would allow a hacker to gain access to such a system. All it affords is a chance to understand the administrative functions a little better. We'd like to assume that any outside interference to a 911 system is impossible. Does Bell South know otherwise? In light of their touchiness on the matter, we have to wonder.

We'd be most interested in hearing from people with more technical knowledge on the subject. What does this whole escapade tell us? Please write or call so the facts can be brought forward.

fun and games

In a bizarre story that's still in the process of unfolding, hackers at a 2600 meeting in New York City were monitored by investigative agents of some sort and then harassed by a mob of police.

During the meetings, we get quite a few phone calls at the payphones from people all over the world. While one of us was on such a call, the strange man in the suit holding a deskphone was first noticed. Nothing unusual there;

Citicorp is just filled with suspicious-looking types.

Citicorp is filled with suspicious and unusual kinds of people. (We fit right in.) But then we managed to overhear what he was saying. He was describing what the people at the meeting looked like!

We started watching him *very* closely. So closely that we're sure he soon realized what a bad undercover investigator he was.

We videotaped him. We took his picture. We recorded his voice. We even tried to be friendly but he got embarrassed and disappeared.

Ten minutes later, close to a dozen cops suddenly materialized

Who was this strange man?
Why was he watching us?
And what was the deskphone for?

This man found a nice post to lean against for two hours.

on the scene. They demanded to know who we were talking to on the phone. Friends, we told them. Then they told us to hang up.

"We know you're pranking 911," one of them said to one of us.

at a 2600 meeting

"Right now we're trying to decide whether or not to lock you up."

Pranking 911? They *had* to be kidding! Maybe a group of five year olds would be doing that, but *not* a group of hackers that knew all about 911 tracing capabilities. More importantly, it was something none of us would ever *want* to do.

We told them this and we asked if they had actually received calls from this location. Did ANI spit out those numbers down at headquarters?

The leader of the cops seemed to get confused at this point and

Close to a dozen cops suddenly materialized.

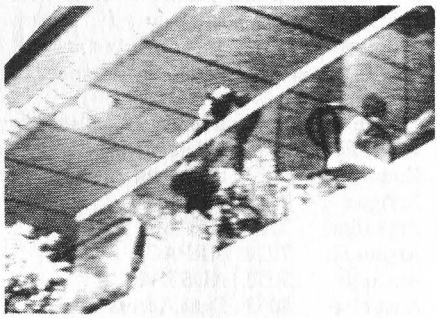
started conferring with some of the others. Then, just as quickly as they had arrived, they left.

What was it all about? We may never know for sure. But we do know that intimidation tactics and frame-ups will ultimately fail.

Incidentally, 2600 meetings take place in the public lobby of Citicorp in New York City (53rd Street between 3rd and Lexington) from 5 to 8 pm on the first Friday of the month. Those payphone numbers are: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162, and 212-308-8184.

The leader of the cops seemed to get confused.

There will be several 2600 meetings in California this summer involving American and Dutch hackers. For more information or to meet up with us while we're over there, call 2600 at 516-751-2600.



Relax, it could be an innocent tourist taking pictures of all the cops.

Data Network Identification Codes

Most X.25 based public data networks around the world are interconnected using the CCITT X.75 protocol. An addressing scheme for global data networks is the X.121 standard. Under this standard, a host address consists of 14 digits.

3110 91400123 01
DNIC NUA PORT

The above example address is the same as 914123.01 on Telenet. The NUA is the Network User Address of the host machine on that network. The DNIC for Telenet is 3110. The PORT is optional and can be excluded because most host machines will "hunt" from port to port.

A DNIC (Data Network Identification Code) is a 4 digit code that is used to identify the network which will connect you to a host machine. A DNIC is used as a prefix before the NUA (Network User Address). The first digit of the DNIC is one of 7 designated world zones.

Using DNIC's is fairly simple. For example, if I was connected to Telenet and wanted to reach a host on the Austrian DATEX-P network I would use:

@ C 2322<NUA>,<NUI>,<PASSWORD>

The NUI and PASSWORD are optional if the host machine is willing to accept collect calls. Your NUI and PASSWORD is your account that you have set up with Telenet. It is very similar to a PC Pursuit account. In fact, if you have a PCP account, you can use that to connect to foreign hosts.

The following is a list of DNIC's along with their countries and networks.

Country	DNIC	Network
Antigua	3443	Aganet
Argentina	7220	ARPAC
Argentina	7222	ARPAC
Australia	5052	AUSPAC
Australia	5053	Data Access
Austria	2322	DATEX-P
Austria	2329	RA
Bahamas	3640	BaTelCo
Bahrain	4263	BAHNET
Barbados	3423	
Belgium	2062	DCS
Bermuda	3503	Bermudanet
Brazil	7240	Interdata
Brazil	7241	Renpac
Canada	3020	Datapac
Canada	3025	Globedat
Canada	3028	CNCP
Canada	3106	Tymnet Canada
Cayman Islands	3463	IDAS
Chile	3104	Entel
Chile	7302	Entel
Chile	7303	Chile-PAC
Chile	7305	VTR
China	4600	PTELCOM
Colombia	3107	DAPAQ
Costa Rica	7122	RACSAPAC
Denmark	2382	Datapak
Dominican Rep	3700	UDTS-I
Egypt	6020	ARENTO
Finland	2442	Datapak
Fr Antilles	3400	Dompac
Fr Guiana	7420	Dompac
France	2080	Transpac
France	2081	NTI
Gabon	6282	Gabonpac
Germany F.R.	2624	DATEX-P
Greece	2022	Helpak
Greenland	2901	KANUPAX
Guam	5351	PCINET
Guatemala	7043	GAUTEL
Honduras	7080	HONDUTEL
Hong Kong	4542	INTELPAK
Hong Kong	4545	DATAPAK
Hungary	2621	DATEXL
Iceland	2740	Icepak
Indonesia	5101	SKDP
Ireland	2724	Eirpac
Israel	4251	Isranet
Italy	2222	Itapac
Italy	2227	Italcable
Ivory Coast	6122	SYTRANPACI
Jamaica	3380	Jamintel
Japan	4401	NTT DDX
Japan	4406	NISnet
Japan	4408	KDD Venus-P

(continued on page 42)

2600 Marketplace

2600 WILL BE HAVING WEST COAST MEETINGS during the month of July. Hackers from Holland will also be there. Call 516-751-2600 to find out where exactly we'll be or to make suggestions as to where we should go.

VMS HACKERS: For sale: a complete set of DEC VAX/VMS manuals in good condition. Most are for VMS revision 4.2; some for 4.4. Excellent for "exploring"; includes System Manager's Reference, Guide To VAX/VMS System Security, and more. Mail requests to Roger Wallington, P.O. Box 446, Leonia, NJ 07605-0446.

WANTED: Red box plans, kits, etc. Also back issues of Phrack, Syndicate Reports, and any other hack/phreak publications, electronic or print wanted. Send information and prices to Greg B., 2211 O'Hara Dr., Charlotte, NC 28273.

TAP MAGAZINE now has a BBS open for public abuse at 502-499-8933. We also have free issues. You send us a 25 cent stamp and we send you our current issue. Fancy huh? Mail to TAP, P.O. Box 20264, Louisville KY 40250-0264.

SUBSCRIBE TO CYBERTEK, a magazine centered upon technology with topics on computer security. Send $10 for a one year subscription to Cybertek Magazine, PO Box 64, Brewster, NY 10509.

NEEDED: Info on speech encryption (Digicom, Crypto). Send to Hack Tic, P.O. Box 22953, 1100 DL, Amsterdam, The Netherlands.

CYBERPUNKS, HACKERS, PHREAKS, Libertarians, Discordians, Soldiers of Fortune, and Generally Naughty People: Protect your data! Send me a buck and I'll send you an IBM PC floppy with some nifty shareware encryption routines and a copy of my paper "Crossbows to Cryptography: Techno-Thwarting the State." Chuck, The LiberTech Project, 8726 S. Sepulveda Blvd., Suite B-253, Los Angeles, CA 90045.

RARE TEL BACK ISSUE SET (like TAP but strictly telephones). Complete 7 issue 114 page set. $15 ppd. Have photo copy machine self-serve key counter. Would like to trade for red box minus its IC'S. Pete Haas, P.O. Box 702, Kent, Ohio 44240.

WANTED: Red box kits, plans, and assembled units. Also, other unique products. For educational purposes only. Please send information and prices to: TJ, 21 Rosemont Avenue, Johnston, RI 02919.

THE CHESHIRE CATALYST, former editor of the TAP newsletter, has dates available to lecture in Europe in late August and early September. For lecture fees and information on seminars to be given, write to: Richard Cheshire, P.O. Box 641, Cape Canaveral, FL, USA 32920.

KEEP WATCHING this space.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

FOR SALE: Manual for stepping switches (c) 1964. This is a true collector's item, with detailed explanations, diagrams, theory, and practical hints. $15 or trade for Applecat Tone Recognition program. FOR SALE: Genuine Bell phone handset. Orange w/tone, pulse, mute, listen-talk, status lights. Fully functional. Box clip and belt clip included. $90 OBO. Please post to S. Foxx, POB 31451, River Station, Rochester, NY 14627.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info Payphone numbers at Citicorp: 212-223-9011,212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184.

Deadline for Summer Marketplace: 7/1/90.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

Data Network Identification Codes

(continued from page 40)

Japan	4410	NI+CI
Korea Rep	4501	DACOM-NET
Kuwait	4263	
Lebanon	4155	SODETEL
Luxembourg	2704	Luxpac
Malaysia	5021	Maynet
Mauritius	6170	MauriData
Mexico	3340	TELEPAC
N. Antilles	3620	
N. Marianas	5351	PCInet
Netherlands	2041	Datanet-1
Netherlands	2049	Datanet-1
New Caledonia	5460	Tompac
New Zealand	5301	Pacnet
Norway	2422	Datapak
Panama	7141	
Panama	7142	INTELPAQ
Peru	3104	IMPACS
Philippines	5151	CAPWIRE
Philippines	5152	PGC
Philippines	5154	GMCR
Philippines	5156	ETPI
Polynesia	5470	Tompac
Portugal	2680	Telepac
Portugal	2682	SABD
Puerto Rico	3300	UDTS-I
Puerto Rico	3301	PRTC
Qatar	4271	DOHPAC
Reunion	6470	Dompac
San Marino	2922	X-NET
Saudi Arabia	4263	Bahnet
Singapore	5252	Telepac
South Africa	6550	Saponet
South Africa	6559	Saponet
Spain	2145	Iberpac
Sweden	2402	Datapak
Switzerland	2284	Telepac
Taiwan	4872	PACNET
Taiwan	4877	UDAS
Thailand	5200	IDAR
Tortola, BVI	3483	
Trinidad	3740	Textel
Trinidad	3745	Datanett
Tunisia	6050	RED25
Turkey	2862	Turpac
Turks BWI	3763	
U. Kingdom	2341	BTI IPSS
U. Kingdom	2342	BT PSS
U. Kingdom	2350	Mercury
U. Kingdom	2352	Hull
U.S. Virgin I	3320	UDTS-I
UAE	3104	IMPACS
UAE	4243	EMDAN
Uruguay	7482	
USA	3106	Tymnet
USA	3110	Telenet
USA	3126	Autonet
USA	3134	Accunet
USA	3135	Alascom
USA	3135	Alaskanet
USA	3139	Netexpress
USSR	2502	Iasnet
Zimbabwe	6482	Zimnet

Here is the same list in DNIC order, to help give you a sense of how the codes are allocated.

DNIC	Network	Country
2022	Helpak	Greece
2041	Datanet-1	Netherlands
2049	Datanet-1	Netherlands
2062	DCS	Belgium
2080	Transpac	France
2081	NTI	France
2145	Iberpac	Spain
2222	Itapac	Italy
2227	Italcable	Italy
2284	Telepac	Switzerland
2322	DATEX-P	Austria
2329	RA	Austria
2341	BTI IPSS	U. Kingdom
2342	BT PSS	U. Kingdom
2350	Mercury	U. Kingdom
2352	Hull	U. Kingdom
2382	Datapak	Denmark
2402	Datapak	Sweden
2422	Datapak	Norway
2442	Datapak	Finland
2502	Iasnet	USSR
2621	DATEXL	Hungary
2624	DATEX-P	Germany F.R.
2680	Telepac	Portugal
2682	SABD	Portugal
2704	Luxpac	Luxembourg
2724	Eirpac	Ireland

(DNIC's) Of The World

2740	Icepak	Iceland
2862	Turpac	Turkey
2901	KANUPAX	Greenland
2922	X-NET	San Marino
3020	Datapac	Canada
3025	Globedat	Canada
3028	CNCP	Canada
3104	Entel	Chile
3104	IMPACS	Peru
3104	IMPACS	UAE
3106	Tymnet	USA
3106	Tymnet	Canada
		Canada
3107	DAPAQ	Colombia
3110	Telenet	USA
3126	Autonet	USA
3134	Accunet	USA
3135	Alascom	USA
3135	Alaskanet	USA
3139	Netexpress	USA
3300	UDTS-I	Puerto Rico
3301	PRTC	Puerto Rico
3320	UDTS-I	U.S. Virgin I
3340	TELEPAC	Mexico
3380	Jamintel	Jamaica
3400	Dompac	Fr Antilles
3423		Barbados
3443	Aganet	Antigua
3463	IDAS	Cayman Islands
3483		Tortola, BVI
3503	Bermudanet	Bermuda
3620		N. Antilles
3640	BaTelCo	Bahamas
3700	UDTS-I	Dominican Rep
3740	Textel	Trinidad
3745	Datanett	Trinidad
3763		Turks BWI
4155	SODETEL	Lebanon
4243	EMDAN	UAE
4251	Isranet	Israel
4263		Kuwait
4263	BAHNET	Bahrain
4263	Bahnet	Saudi Arabia
4271	DOHPAC	Qatar
4401	NTT DDX	Japan
4406	NISnet	Japan
4408	KDD Venus-P	
		Japan
4410	NI+CI	Japan
4501	DACOM-NET	
		Korea Rep
4542	INTELPAK	Hong Kong
4545	DATAPAK	Hong Kong
4600	PTELCOM	China
4872	PACNET	Taiwan
4877	UDAS	Taiwan
5021	Maynet	Malaysia
5052	AUSPAC	Australia
5053	Data Access	Australia
5101	SKDP	Indonesia
5151	CAPWIRE	Philippines
5152	PGC	Philippines
5154	GMCR	Philippines
5156	ETPI	Philippines
5200	IDAR	Thailand
5252	Telepac	Singapore
5301	Pacnet	New Zealand
5351	PCINET	Guam
5351	PCInet	N. Marianas
5460	Tompac	New Caledonia
5470	Tompac	Polynesia
6020	ARENTO	Egypt
6050	RED25	Tunisia
6122	SYTRANPACI	
		Ivory Coast
6170	MauriData	Mauritius
6282	Gabonpac	Gabon
6470	Dompac	Reunion
6482	Zimnet	Zimbabwe
6550	Saponet	South Africa
6559	Saponet	South Africa
7043	GAUTEL	Guatemala
7080	HONDUTEL	
		Honduras
7122	RACSAPAC	Costa Rica
7141		Panama
7142	INTELPAQ	Panama
7220	ARPAC	Argentina
7222	ARPAC	Argentina
7240	Interdata	Brazil
7241	Renpac	Brazil
7302	Entel	Chile
7303	Chile-PAC	Chile
7305	VTR	Chile
7420	Dompac	Fr Guiana
7482		Uruguay

the 707 area code

by Lurch

The following is a list of all exchanges for area code 707, which runs from the north end of San Francisco Bay to the Oregon border along the wild, windy North Coast of California. This could be useful if you're looking for "hidden" exchanges, ANI, ring-back, PacTel test numbers, or just modem tones here in Sillycon Valley North.

Pop and org centers are (in no special order) Santa Rosa, Petaluma, Fairfield-Suisun, Eureka, Vacaville, Vallejo, Napa, and Benecia. County codes are: NA (Napa), ME (Mendocino), LA (Lake), SA (Sonoma), MA (Marin), HU (Humboldt), DN (Del Norte), TR (Trinity), and SO (Solano).

224	NA	Napa
226	NA	Napa
247	ME	Piercy
252	NA	Napa
253	NA	Napa
255	NA	Napa
257	NA	Napa
258	NA	Napa
263	LA	Lakeport
270	SA	Santa Rosa
274	LA	Nice
275	LA	Upper Lake
277	LA	Kelseyville
279	LA	Kelseyville
374	SO	Rio Vista
422	SO	Fairfield-Suisun
423	SO	Fairfield-Suisun
424	SO	Fairfield-Suisun
425	SO	Fairfield-Suisun
426	SO	Fairfield-Suisun
427	SO	Fairfield-Suisun
428	SO	Fairfield-Suisun
429	SO	Fairfield-Suisun
431	SA	Healdsburg
433	SA	Healdsburg
437	SO	Fairfield-Suisun
442	HU	Eureka
443	HU	Eureka
444	HU	Eureka
445	HU	Eureka
446	SO	Vacaville
447	SO	Vacaville
448	SO	Vacaville
449	SO	Vacaville
457	DN	Crescent City
458	DN	Crescent City
468	ME	Ukiah
482	DN	Klamath
485	ME	Ukiah
487	DN	Smith River
488	HU	Orick
523	SA	Santa Rosa
525	SA	Santa Rosa
526	SA	Santa Rosa
527	SA	Santa Rosa
528	SA	Santa Rosa
538	SA	Santa Rosa
539	SA	Santa Rosa
542	SA	Santa Rosa
545	SA	Santa Rosa
546	SA	Santa Rosa
552	SO	Vallejo
553	SO	Vallejo
554	SO	Vallejo
557	SO	Vallejo
571	SA	Santa Rosa
573	SA	Santa Rosa
574	TR	Mad River
574	SA	Santa Rosa
575	SA	Santa Rosa
576	SA	Santa Rosa
577	SA	Santa Rosa
578	SA	Santa Rosa
579	SA	Santa Rosa
584	SA	Santa Rosa
585	SA	Santa Rosa
586	SA	Santa Rosa
629	HU	Petrolia
632	SA	Cazadero
642	SO	Vallejo
643	SO	Vallejo
644	SO	Vallejo
645	SO	Vallejo
646	SO	Vallejo
648	SO	Vallejo
664	SA	Petaluma-Rohnert Park
668	HU	Blue Lake
677	HU	Trinidad
722	HU	Pepperwood
725	HU	Fortuna
733	HU	Loleta
743	ME	Potter Valley
744	ME	Hopland
745	SO	Benecia
746	SO	Benecia
747	SO	Benecia
762	SA	Petaluma
763	SA	Petaluma
764	HU	Rio Dell (Scotia)
765	SA	Petaluma
768	HU	Hydesville
777	HU	Bridgeville
778	SA	Petaluma
785	SA	Timber Cove
786	HU	Ferndale
792	SA	Petaluma
794	SA	Petaluma
795	SA	Petaluma
822	HU	Arcata
823	SA	Sebastapol
826	HU	Arcata
829	SA	Sebastapol
833	SA	Kenwood
838	SA	Windsor
839	HU	Arcata
847	SA	Timber Cove
857	SA	Geyserville
864	SO	Fairfield-Suisun
865	SA	Monte Rio
869	SA	Guemeville
874	SA	Occidental
875	SA	Bodega Bay
876	SA	Valley Ford

(continued on page 46)

BOOK REVIEW

The Cuckoo's Egg
By Clifford Stoll
Published by Doubleday
$19.95, 326 pages
ISBN 0-385-24946-2

Review by Dr. Williams

Anybody who's somebody nowadays seems to write a book. Whether it's a celebrity, athlete, or entrepreneur, they all want to tell their story. Clifford Stoll is no exception to this latest craze. In a release by Doubleday, Stoll shares all of his experiences while employed at Berkeley Labs.

In case you might have missed one of Stoll's written articles, TV interviews, or lecture circuit appearances, *The Cuckoo's Egg* is about a year-long effort to apprehend Mark Hess. Hess was a West German hacker breaking into computers all over Europe, North America, and Japan through a tangled web of computer networks. Until his capture, Stoll watched Hess attempt to break into over 400 computer sites on Milnet and Arpanet. Hess was successful in about 40 of his attempts.

Stoll first became aware of the hacker's presence when he discovered a 75 cent accounting error in the Unix system he was administering. One thing led to another, and he realized an unauthorized user was on his system. Instead of getting rid of the account and locking out the hacker, Stoll methodically kept notes and records on the hacker's every move. Stoll alerted all the government agencies that he thought could act upon the case. He started performing traces with the help of Tymnet, a data carrier on which Hess was placing his calls.

As his activities grew, the more interest government agencies showed in Hess. It became apparent the hacker was coming from Europe and showed a strong taste for documents concerning the Star Wars project. The slow wheels of bureaucracy started to move. The FBI, the only agency with the authority to act on the case, officially asked for help from West Germany. With their help, the FBI was able to quickly clamp down on the identity of the hacker. He was arrested nearly one year after Stoll first discovered the accounting error in his system.

The Cuckoo's Egg excels in giving detail into the inner workings of the people involved in capturing Mark Hess. Stoll provides all of the glorious detail of all the agencies involved in the case, what their role was, what their response was to the intrusions, and what their actions were. He tells what the CIA said and did, as well as the NSA and FBI. Everybody's role and their relevance to the case is discussed.

The Cuckoo's Egg provides excellent advice for any network hacker. Stoll explains what traces took place, how long they took to perform, and what the stumbling blocks were in catching the hacker. Stoll tells how many system administrators knew their systems were actually being attacked. If the hacker did succeed in penetrating the system, Stoll describes how many system administrators realized it and what they did once they found out. By seeing the strong and weak spots of system operators and nets, a network hacker is more able to act in a manner which is prudent to his security, while making him aware of more opportunities.

Stoll mentions the techniques used by the hacker to gain access to a sys-

tem, and the security flaws exploited. The security flaws are not described in detail, but anyone familiar with the computer systems mentioned should already be aware of them.

The Cuckoo's Egg does take Stoll's reactions a bit too far at times. Stoll says the hacker managed to break into an account when all the hacker did was log into a guest account. (Account name: Guest or Anonymous. No password.) He fails to consider that these accounts are set up precisely for guests, regardless of whether or not they log in for malicious reasons.

Stoll also makes too big a deal out of old security holes. He is shocked to learn the Gnu-Emacs holes, which go back to the early 80's (see some of the TAP issues). The X-Preserve hole for the vi editor is another discovery to Stoll, even though that hole is equally well known. Stoll's real shock comes at learning that anybody can take a public readable encrypted password file, and use the same password encryption scheme as the host computer to make dictionary guesses at passwords. This method is perhaps the oldest of them all.

The Cuckoo's Egg also suffers in part from its "novelist" approach at times. Perhaps as a way to stretch out the material, the book is full of irrelevant aspects of Stoll's life and thoughts which have nothing to do with the matter at hand. He constantly bores the reader with personal interactions between him and his wife-to-be, describes how he spent Halloween, Christmas, and every other day, and continually interjects his own "cutesie" observations of life. Stoll also brings back so many immaterial analogies and stories from his grad school days that the reader would think he spent the better part of eight years just to get his master's degree. Most hackers reading the book could hardly give a rip about Stoll's personal life.

From the security standpoint, *The Cuckoo's Egg* stands alone. No other book goes into the gripping detail of the operations used to catch Mark Hess. To Stoll's credit, he kept a detailed lab book of every activity, conversation, and contact during the entire affair. His notes made for an accurate retelling. Any hacker working on a net would benefit from reading this book by learning about the weak spots in the networks as well as how to avoid being tracked down as Mark Hess was.

---

707 *(continued from page 44)*

877	ME	Elk
878	MA	Tomales
882	ME	Point Arena
884	ME	Gualala
886	SA	Annapolis
887	SA	Forestville
894	SA	Cloverdale
895	ME	Boonville
923	HU	Garberville
925	ME	Leggett
926	HU	Alderpoint
928	LA	Cobb Mountain
935	SA	Sonoma
937	ME	Mendocino
938	SA	Sonoma
942	NA	Calistoga
943	HU	Miranda (Myers Flat)
944	NA	Yountville
946	HU	Weott
961	ME	Fort Bragg
963	NA	St. Helena
964	ME	Fort Bragg
965	NA	St. Helena
966	NA	Lake Berryessa
967	NA	St. Helena
983	ME	Covelo
984	ME	Laytonville
986	HU	Whitethorn
987	LA	Middletown
994	LA	Lower Lake
995	LA	Lower Lake
996	SA	Sonoma
998	LA	Clearlake Oaks

Only ONE exchange in the entire area code that begins with 3? We suspect THAT might be a good place to go hunting.

IT'S EASY

In fact, it's never been easier to renew your subscription to 2600. Just look at your mailing label to find out when your last issue will be. If you have two or fewer issues remaining, it's probably a good idea to renew now and avoid all the heartache that usually goes along with waiting until your subscription has lapsed. (We don't pester you with a lot of reminders like other magazines.) And by renewing for multiple years, you can cheerfully ignore all of the warnings (and occasional price increases) that appear on Page 47.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

TOTAL AMOUNT ENCLOSED:

take a look

for your protection	3
facts about mizar	8
how blue boxers are caught	12
build a touch tone decoder	14
listening in via vhf	19
news update	23
letters	24
the 911 document	37
fun at the 2600 meeting	38
dnic codes	40
2600 marketplace	41
the 707 area code	44
the cuckoo's egg	45

SECOND CLASS POSTAGE

Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

$LOD^2 < 1300$

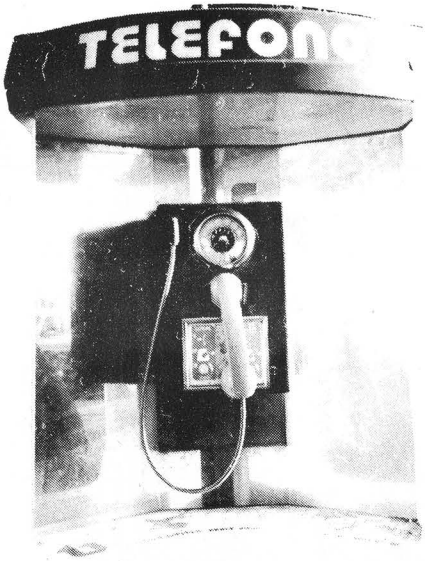
2600

5

The Hacker Quarterly

VOLUME SEVEN, NUMBER TWO
SUMMER, 1990

MEXICAN PAYPHONES



SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES,
PO BOX 99, MIDDLE ISLAND, NY 11953.

Due to a satellite error, a couple of pictures we printed on page 38 of our last issue were jumbled. In order to keep the record straight, we wish to make it absolutely clear that this was the person who was spying on us on behalf of God knows who.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1990, 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESS: 2600@well.sf.ca.us.

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

A BITTERSWEET VICTORY

By now a good many of you have probably heard the news about the *Phrack* case we talked about in the last issue. In case you haven't, the charges were officially dropped when it became clear that Bell South had provided false information to the prosecution. The document they claimed to be worth nearly $80,000 turned out to be obtainable from them for a mere $13. In an unprecedented move, the superiors of the prosecutor involved demanded that he drop the case immediately. Good news, right?

Well, sort of. It's great that one of the publishers of *Phrack* won't be going to jail for putting out a newsletter. But we won't soon be seeing another issue of *Phrack*. As Craig Neidorf tells us in this issue, the risks of running *Phrack* at this stage are far too great. Plus he's got a lot of recovering to do. Legal fees of over $100,000 plus the emotional stress of facing many years in prison for being a publisher...it's a bit much for anyone. So the government managed to shut down *Phrack* and give the publisher a hefty penalty. Not bad, considering they lost the case.

Add to this the fact that there are many other cases pending, cases which are disturbing even to those who know nothing about hacking. Raids are commonplace, as is the misguided zeal of federal prosecutors, who seek to imprison teenagers, hold them at gunpoint, confiscate all kinds of equipment, and put their families through a living hell.

We have a lot of education ahead of us. Much of it will involve getting through to non-hackers to point out the serious dangers of a legal system gone mad. A good part of this issue is devoted to these matters and, as a result, many articles we were planning on running were bumped to the autumn edition. It would be nice if there was substantially less of this to report for our next issue.

the neidorf/phrack trial:

by Gordon Meyer and Jim Thomas

"The Government screwed up!" "Bill Cook pulled his head out!" "The computer underground will live forever!"

These comments, and undoubtedly countless others, have been echoing throughout the computer underground (C.U.) ever since the surprise announcement on July 27 that the Government was withdrawing from the prosecution of Craig Neidorf and *PHRACK Magazine* (see Spring 90 issue). What follows is a full accounting of the events of this five day trial.

The Trial: Day by Day

Day One (July 23): The jury selection in case # 90 CR 70 (United States v. Craig Neidorf) was completed on the first day. Although opening statements were also scheduled to begin that day, the selection of jurors, while not overly arduous, did perhaps take longer than was anticipated. Courtroom observers were overheard remarking that Judge Bua seemed to be a bit more cautious and in-depth in his questioning than usual.

The government was represented by a team of three attorneys, headed by Bill Cook. Also in attendance was Agent Foley of the U.S. Secret Service. Defendant Neidorf, dressed in a blue blazer and khaki pants, was seated next to his attorney, Sheldon Zenner. Also in attendance, though seated in the gallery, were Craig's parents, his grandparents, expert witnesses Dorothy Denning and John Nagle (scheduled to testify later in the trial), and several other lawyers and staff from Katten, Muchin, and Zavis (the firm with which Zenner is associated).

Bua's opening remarks to the prospective jurors included a brief summary of the charges and an admonishment that an indictment does not necessarily translate into guilt. Bua's questions to each of the jurors, after they were called to sit in the jury box for consideration, included the traditional "where do you live" and "what magazines do you subscribe to" questions, but also included specific inquiries into grievances or affiliation with Bell South/AT&T/Illinois Bell, association with Craig's college fraternity (ZBT), and use/knowledge of computers. Jurors were also queried as to whether or not they had any idea what a computer bulletin board was, and if they had ever used one.

The process of juror selection took over four hours and thirty minutes (excluding recesses). During this time several people were excused from the selection pool for various reasons. In federal court the judge queries the jurors, with the counsel for each party communicating their "vote" via written messages. Therefore, it is difficult to say for sure whether the defense or prosecution wished to exclude which individuals. (It is also possible that a potential juror was excluded for other reasons, such as knowing a witness, etc.) Nevertheless, it seemed quite obvious why some people were not chosen. A few, for example, turned out to be Bell South and/or AT&T stockholders. Another had a husband who worked for Motorola Cellular (which has ties to Bell South Mobile). One man had served on three juries and one grand jury previously. And finally there was a Catholic priest who had studied constitutional law, been involved in an ACLU sponsored lawsuit against the state of Colorado, and been involved in various other litigations.

Here is a thumbnail sketch of each jury member that was selected. (The first six were selected and sworn in before lunch, the next six and the alternates that afternoon.) The information here has been gleaned from their selection interviews and is presented so as to get a better idea of who the "peers" were that would have judged Craig.

1. Male, white, mid to late 20's. Works in an orthopedic surgeon's office. Has computer experience in using SPSSx-PC, 1-2-3, and various other number-crunching applications. Doesn't subscribe to any magazines.

2. Elderly white female. Retired, but used to work at a Hallmark store. No computer experience.

3. Female, white, mid to late 40's. Teaches court reporting at a trade school, has never worked as a court reporter. Has some computer experience with word processing and spreadsheets.

4. Female, white, middle aged. Former City Clerk (elected) of a Chicago suburb. No computer experience. Subscribes to *Readers' Digest*.

5. Male, White, late 30's. Passenger pilot for American Airlines. Subscribes to *Compute! Magazine*. Has a PC at home. The only juror to have ever used a BBS (one set up by American for use by the pilots).

6. Female, Afro-American. Works as a school volunteer and a babysitter. Has used history teaching programs on Apple PC's at Malcolm X College.

7. Female, Afro-American. Works in claims underwriting at CNA. Experience in word processing

and using LAN based PC's. Former Illinois Bell and AT&T employee.

8. Female, Afro-American. Works for the Chicago Board of Education. Some computer experience in the classroom (as a teaching tool). Holds an MS degree in Special Ed.

9. Female, white, elderly. School teacher (1st grade). Classroom use of computers. MA degree in education. Subscribes to *Newsweek.*

10. Male, Afro-American, 36 years old. Lives with parents who are retired postal workers. Employee of Trans-Union credit reporting company. Programming exposure in BASIC and COBOL.

11. Female, white, early 20's. Lives with parents. Holds a BA in education, studying for a masters from North Western University. Teaches junior high, has WP and some DTP use of computers but limited in other knowledge.

12. Male, white, 30-ish. Chief engineer at a company that makes floor trusses for construction sites. Has a BS in architectural engineering. Has done a little programming. Uses CAD packages, spreadsheets. Had a class in FORTRAN in college. Has used a modem to download files from software manufacturers.

Alternate Jurors

1. Female, white. Works as a systems analyst and LAN administrator. Familiar with PC to mainframe connections. Holds a BA in Special Education and has about 20 hours of computer classes. Familiar with assembler, COBOL, and PL1 among other languages.

2. Female, white. Owns and operates a small hotel with her husband. Uses a Macintosh for word processing but husband does most of the computer stuff. Holds a BA from Northwestern. Subscribes to the *New York Times.*

3. Female, Afro-American. Works at the Christian League of Chicago. Formerly a word processor at Montgomery Wards.

4. Male, white, early 50's. Elementary school principal. Former phys-ed teacher. Accessed school district records using modem connection to district computer, has used e-mail on the district's bulletin board. Holds an MA in Education from Loyola University of Chicago.

Random Notes: Although Judge Bua was careful to pronounce each of the prospective juror's last names correctly, he seemed to mispronounce Neidorf's name differently every time he said it. "Neardorf", "Neardof", and "Nierndon" were distinctly heard. Bill Cook and Agent Foley also continually mispronounced the name, and it was misspelled on at least one prosecution evidence chart.

Finally, a reporter from Channel 7 in Chicago was in and out of the courtroom throughout the day. Reportedly a brief piece ran on the evening news in Chicago.

Day Two (July 24): On the second day of Craig Neidorf's trial in Chicago, both sides presented their opening arguments. The prosecution wheeled in two shopping carts containing documents, presumably to be used as evidence. Bill Cook, the prosecutor, downplayed the technical aspects of the case and tried to frame it as a simple one of theft and receiving/transporting stolen property. Sheldon Zenner's opening statements were absolutely brilliant, and challenged the definitions and interpretations of the prosecution.

Day Three (July 25): The prosecution continued presenting its witnesses. The most damaging to the prosecution (from a spectator's perspective) was the testimony of Billie Williams from Bell South whose primary testimony was that the E911 documents in question were a) proprietary and b) not public information. Following a lunch break, defense attorney Sheldon Zenner methodically, but politely and gently, attacked both claims. The "proprietary" stamp was placed on *all* documents at the source without any special determination of contents and there was nothing necessarily special about any document with such a statement attached. It was established that it was a bureaucratic means of facilitating processing of documents. The proprietary claims were further damaged when it was demonstrated that not only was the content of E911 files available in other public documents, but that the public can call an 800 number and obtain the same information in a variety of documents, including information dramatically more detailed than any found in *PHRACK.* After considerable waffling by the witness, Zenner finally received her acknowledgement that the information found in the files presented as evidence could be obtained for a mere $13, the price of a single document, by simply calling a public 800 number to Bellcore, which provided thousands of documents, "including many from Bell South." If our arithmetic is correct, this is a little less than the original assessed value of $79,449 in the original indictment, and about $22,987 less than the revised value assessed in the second document.

the neidorf/phrack trial:

Ms. Williams often seemed hesitant and uncooperative in answering Zenner's questions, even simple ones that required only a "yes" or a "no". For example, part of Ms. Williams' testimony was the claim that *PHRACK's* E911 document was nearly identical to the original Bell South document, and she noticed only four changes in the published text. Zenner identified other differences between the two versions. He then suggested that it was odd that she didn't notice that the original document was about 24 pages and the *PHRACK* document half of that. He wondered why she didn't notice that as a major change. She tried to avoid the question, and in exasperation, Zenner gently asked if she didn't think that to reduce 24 pages to about 13 indicated a major editing job: "Doesn't that indicate that somebody did a good job of editing?" "I don't know what you mean." After a bit of banter in which Zenner tried to pin down the witness to acknowledge that a major editing had occurred such that the *PHRACK* document was hardly a facsimile of the original, and several "I don't know's" from the witness, Zenner turned to her and said gently: "Editing. You know, that's when somebody takes a large document and reduces it." "I don't know," she repeated again. This seemed especially damaging to the prosecution, because they had claimed that the document was nearly identical. In challenging a motion to dismiss, the prosecution had written:

"Neidorf received and edited the file and subsequently, on January 23, 1989, uploaded a "proof copy" of the edited text file onto Riggs' file area on the Lockport bulletin board for Riggs to review. (Counts 8 and 9). Riggs was to proofread Neidorf's version before Neidorf included it in an upcoming issue of *PHRACK*. The only differences between the original version posted by Riggs, and the edited version that Neidorf posted for return to Riggs, were that Neidorf's version was retyped and omitted all but one of the Bell South proprietary notices contained in the text file. Neidorf modified the one remaining Bell South warning notice by inserting the expression "whoops" at the end:

NOTICE: NOT FOR USE OR DISCLOSURE OUTSIDE BELL SOUTH OR ANY OF ITS SUBSIDIARIES EXCEPT UNDER WRITTEN AGREEMENT. [WHOOPS]"

Also in the afternoon session, Secret Service Special Agent Timothy Foley, in charge of the search of Craig Neidorf and others, related a detailed account of the search and what he found. A number of files from *PHRACK* and several e-mail messages between Craig and others were introduced as government exhibits. In addition to the E911 files, the following were introduced:

PHRACK Issue 21, File 3; *PHRACK* Issue 22, File 1; *PHRACK* Issue 23, File 1; *PHRACK* Issue 23, File 3; *PHRACK* Issue 24, File 1; *PHRACK* Issue 24, File 11; *PHRACK* Issue 25, File 2.

From a spectator's perspective, the most curious element of Agent Foley's testimony was his clear presentation of Craig as initially indicating a willingness to cooperate and to talk without a lawyer present. Given the nature of the case, one wonders why the government couldn't have dealt less aggressively with this case, since the testimony was explicit that, had it been handled differently, justice could have been served without such a waste of taxpayer dollars. When Agent Foley read the *PHRACK* file describing Summercon, one was also struck by what seemed to be little more than an announcement of a party in which there was explicit emphasis on informing readers that nothing illegal would occur, and that law enforcement agents were also invited.

It was also curious that, in introducing the PHRACK/INC Hacking Directory, a list of over 1,300 addresses and handles, the prosecution found it important that LoD participants were on it, and made no mention of academics, security and law enforcement agents, and others. In some ways, it seemed that Bill Cook's strategy was to put *hacking* (or his own rather limited definition of it) on trial, and then attempt to link Craig to hackers and establish guilt by association. It was also strange that, after several months of supposed familiarization with the case, neither Bill Cook nor Agent Foley would pronounce his name correctly. Neidorf rhymes with eye-dorf. Foley pronounced it KNEEdorf and Cook insisted on NEDD-orf. Further, his name was spelled incorrectly on at least three charts introduced as evidence, but as Sheldon Zenner indicated, "We all make mistakes." Yeah, even Bill Cook. One can't but think that such an oversight is intentional, because a prosecutor as aware of detail as Bill Cook surely by now can be expected to know who he is prosecuting, even when corrected. Perhaps this is just part of a crude, arrogant style designed to intimidate. Perhaps it is ignorance, or perhaps it is a simple mistake. But, we judge it as an offense both to Craig and his family to sit in the courtroom and listen

to the prosecutor continually and so obviously mispronounce the family name.

Day Four (July 28): Special Agent Foley continued his testimony, continuing to describe the step by step procedure of the search, his conversation with Craig, what he found, and the value of the E911 files. On cross-examination, Agent Foley was asked how he obtained the original value of the files. The value is crucial, because of the claim that they are worth more than $5,000. Agent Foley indicated that he obtained the figure from Bell South and didn't bother to verify it. Then he was asked how he obtained the revised value of $23,000. Again, Agent Foley indicated that he didn't verify the worth. Because of the importance of the value in establishing applicability of Title 18, this seemed a crucial, perhaps fatal, oversight.

Next came the testimony of Robert Riggs (The Prophet), testifying presumably under immunity and, according to a report in *CuD*, under the potential threat of a higher sentence if he did not cooperate. The diminutive Riggs said nothing that seemed harmful to Craig, and Zenner's skill elicited information that, to an observer, actually seemed quite beneficial. For example, Riggs indicated that he had no knowledge that Craig hacked, had no knowledge that Craig ever traded in or used passwords for accessing computers, and that Craig never asked him to steal anything for him. Riggs also indicated that he had been coached by the prosecution. The coaching even included having a member of the prosecution team play the role of Zenner to prepare him for cross-examination. It was also revealed that the prosecution asked Riggs to go over all of the back issues of *PHRACK* to identify any articles that may have been helpful in his hacking career. Although it may damage the egos of some *PHRACK* writers, Riggs identified only one article from *PHRACK* 7 that *might possibly* have been helpful.

Day Five (July 27): After discussion between the prosecution and defense, the judge on Friday declared a mistrial. Although the charges were not, according to sources, formally dropped, the result was the same. All parties are prohibited from discussing the details of the arrangement worked out. But, in essence, Craig was not required to plead guilty to any of the counts and, if he stays out of computer-related trouble for a year, the government cannot re-file the charges.

The arrangement does not prohibit him from associating with whom he pleases, place travel restrictions on him, or prohibit him from editing any newsletter of his choice. He is required to speak to a pre-trial officer for a year (this can be done by telephone), and he in no way was required to give information about others. He will resume school this fall and hopes to complete his degree within about three semesters.

Credit Applications

While some self congratulatory back-slapping and "thumb-nosing" of the feds is expected (and deserved), some kudos need to be shared on both sides of the contest.

To the defense: Dorothy Denning and John Nagle were instrumental in identifying the flaws in the government's case. Their ability to disregard all of the posturing (mostly by supporters on both sides) and focus on the technological and practical side of the charges was superb. But it was Neidorf's attorney, Sheldon Zenner, who was able to quickly integrate and translate the ammunition supplied by Denning and Nagle into the fatal weapons that finally convinced the government to drop the charges. While Zenner's experience as a former Assistant U.S. Attorney was assuredly helpful, his skills in assimilating technical information and applying it in ways that non-technoids could understand was remarkable. And this, from an attorney who is reportedly not all that computer literate himself, although he seems to have learned much since taking this case.

Acknowledgment should also go to Neidorf's family, and to Craig for sticking through the ordeal and not agreeing to plea-bargains or other deals that may have been offered.

Special recognition should go to the efforts of Emmanuel Goldstein and *2600 Magazine* for the editorial in the spring issue, and to the prodding Emmanuel did in *Telecom Digest*, *The Well*, and other places. Pat Townson of *Telecom Digest*, despite his personal views, publicized the issues and allowed Craig's supporters to raise a number of critical points. Finally, *Computer Underground Digest* circulated a number of editorials and samples of the evidence to corroborate claims that Craig's indictment was exaggerated. Together, these and others who spoke out created the visibility that eventually contributed to the formation of the Electronic Frontier Foundation (see story page 10).

But let us not forget the prosecution. The U.S. Attorney's office should be acknowledged, as Zenner and Neidorf have done, for "doing the right thing" and

(continued on page 40)

an interview with

Did you ever believe that you might actually go to prison for publishing the 911 article?

Yes, there was the possibility that I could go to prison because of the federal sentencing guidelines that applied to the charges. Furthermore, I was told by the prosecution that they would be asking for at least two years.

Were you prepared to go to jail?

Yes, especially when the plea bargain was offered. I was prepared to go to jail continuing to proclaim my innocence rather than plead to something I didn't do. I knew the possibility was there. But I guess I didn't really believe it could happen. I knew I was right. And I also, especially in light of the Morris trial, I didn't see how they could ever put someone like me away.

Most people would have gone for a plea bargain of some sort to avoid the ordeal and expense of a trial. But you didn't. Why?

Essentially, on the 26th of July the plea bargain was offered. Had it been offered back in February or March, maybe I would have gone for it back then. But [during the trial] their case was falling apart. And we knew it. They knew it. I think they knew we knew it. But I was prepared to risk it just because I knew our defense strategy. And there was one thing the government had done for me that was better than us trying to establish it ourselves: they had given me credibility. Their own witnesses had testified to the fact that I had never broken into any systems and had been fully cooperative with them. Because of this, I felt that if I took the stand, and I probably was going to, they would believe what I had to say.

Were First Amendment issues ever raised at the trial?

They were mentioned in the opening arguments. But the trial never got to the point of debating the First Amendment. A few comments were made.

What is your opinion of the current "witchhunt" against hackers?

When I was raided, I was not physically abused, as I've heard a lot of other people were. The search warrants they had only allowed them to search one room in the entire fraternity house. Therefore, as long as I wasn't in that room there would be no reason to restrain me. That and the fact that 40 people were watching. But all this running into people's homes and carting off all of this extra equipment seems to be more of a persecution than a prosecution. And it looks like it'll continue for a while until they go that one extra step too far and somebody decides to do something about it.

What kind of a toll has this taken on your personal life?

Well, it wasn't easy. It's caused me to lose a lot of credit hours in school, which ultimately is going to force me to put off law school for at least a full year. It sort of alienated me from a lot of people: some friends who didn't want to get involved and whose parents had made them refrain from having any kind of contact with me. It forced me to break off relations with my best friend [and Phrack co-publisher] although we're back in contact now that the trial is over. But more than that, it just had a great emotional toll on me. I couldn't concentrate on my remaining courses. Every day was something new and it was never good. I was travelling to either St. Louis or Chicago almost every weekend. I didn't have a summer this year and I never really got a break from it.

Has it gotten better?

Immediately after it ended there was a lot of press and people doing interviews with me. You get to be on a sort of high because of all the publicity and the excitement of the aftermath. But as time goes on I'm becoming old news, you might say. It's sort of a downer in that respect. I just have to go back and hit school with everything I've got. But the money situation has gotten pretty bad. I used to have a decent college fund, enough to get me through undergrad. Maybe kick me off into my first year of law school. No longer. I don't have a whole lot of savings after this.

Several media reports implied that your case would receive funding from the newly formed Electronic Frontier Foundation. Has this happened and to what degree? What kind of expenses are remaining?

When I read the first articles about the EFF, I was under the impression that this organization would see the constitutional issues and understand that I was not really financially able to fight this battle. It seemed that they would come through and would actually fund this court battle. As I later found out, it was not their intention to actually provide monetary funding to me. They had paid for court motions filed by their law firm on my behalf concerning the First Amendment. And I guess they got me some good press for a while.

How much are we talking about in terms of what you owe for legal expenses?

We still haven't received the final bill. I'm told that the bill actually reached over $200,000 but that the law firm had found ways to reduce $100,000 off the bill. My parents and I have paid $35,000 to the firm already and an additional $8,000 went to the first law firm we retained in St. Louis which, believe me, was not well spent money. I imagine that we have roughly $65,000 left to pay off.

What are the plans for Phrack?

craig neidorf

I don't have any plans for Phrack, partially because of my studies, but mostly because I can't afford to risk the possibility of being prosecuted because of something that might appear in the newsletter. I just couldn't afford it, financially or emotionally.

What would you say to those people who think this means the government has won and has managed to shut down your magazine?

I'd say that's probably an accurate assessment.

Would you approve of another publication taking over the name of Phrack?

I'm totally against it. I've spoken with the individual responsible for putting out a magazine named Phrack that came out this summer. He's agreed not to release any more issues under the name of Phrack. Whether he holds to this, I don't know. My opinion is that Phrack was something special and it should just be left alone, rather than see someone else continue it and do a shoddy job.

How has this whole chain of events changed your outlook on the hacking world? Is it capable of banding together under adverse circumstances?

I found an extreme amount of support for me from the modem community and a lot of the Phrack subscribers. When I needed help trying to locate people or copies of documents, they were there for me. They were also able to stir up enough exposure about this so that the traditional media sources got involved. I'd say it could have been a very different ending without their help.

What about the media? Is there a way to make sure the facts are presented correctly?

This is not the first time I've seen stories that reporters have gotten completely screwed up. I think it's a fact of life. As people who aren't directly involved in a situation they're not going to be able to relate to it or even understand it in the first place. Then their editor may not be able to understand it. It's really unfortunate. I don't think any story you see printed in the paper really presents the facts accurately. It's like a house of mirrors in a carnival. The images have got all the same parts and colors as the shirt you're wearing. But they're out of proportion.

You've presented yourself as the publisher of a hacker magazine, not a hacker. How important was this distinction?

To the extent that the definition at the trial was that a hacker was a person who illegally broke into systems, then I did not fit under that definition. So it was a very important distinction.

Do you feel this was an accurate definition?

Considering that I believe that a hacker is just a person who has a deep interest in finding uses for computers and ways to use them and work with them, then I'd say that I'm just as much a hacker today as I ever was. But I don't do anything illegal.

Is there a message you'd like to give to all of the hackers out there?

Don't let this scare you too much. It wasn't pleasant by any means. It's not something you want to have happen to you. Natural curiosity existed long before the computer was invented. It's something that you just can't eradicate. One thing I've learned from this is that being cooperative helped me tremendously at the trial. They asked me general questions and I didn't try to hide anything. But it's also possible that if they hadn't taken everything I said and manipulated it, perhaps there wouldn't have been enough to get me indicted in the first place. So I wouldn't say that it's necessarily all right to talk to these people if you have nothing to hide. I was tormented by things I had told them because of the way they interpreted it. It's not what you say, it's what they make out of it. For anyone else who gets a visit, don't lie to these people. But don't talk to them either, no matter how innocent you are. Get an attorney. I don't know if it would have saved me any trouble but at least they can't really make anything out of that because that's just a reasonable thing to do.

To the hackers out there, I say fight for what you believe in. Obviously you don't want to jump in a situation and defend something you don't know enough about. You might be made to look foolish and you may find that you're wrong. I was defending the right to information. And I nearly went to jail for it. I hope that more people are prepared to fight as I was. When you accept a plea bargain on something this new, you're setting a precedent that's going to affect people down the road. Especially here, where they're going after kids who don't have the financial resources to defend themselves. Technically, I don't either. Had I plea bargained something out or plead guilty to something because it was the only thing to do financially, it would have set a precedent that could have done a lot of damage to other people in the future.

WHAT IS THE EFF?

One of the results of our public outcry over the hacker raids this spring has been the formation of the Electronic Frontier Foundation (EFF). Founded by computer industry giants Mitch Kapor and Steve Wozniak along with writer John Barlow, the EFF sought to put an end to raids on publishers, bulletin board operators, and all of the others that have been caught up in recent events. The EFF founders, prior to the organization's actual birth this summer, had said they would provide financial support to those affected by unjust Secret Service raids. This led to the characterization of the group as a "hacker defense fund" by the mainstream media and their condemnation in much of the computer industry.

As a result, when the EFF was formally announced, the organizers took great pains to distance themselves from computer hackers. They denied being any kind of a defense fund and made a nearly $300,000 donation to Computer Professionals for Social Responsibility (CPSR).

"We are helping educate policy makers and the general public," a recent EFF statement said. "To this end we have funded a significant two-year project on computing and civil liberties to be managed by CPSR. With it, we aim to acquaint policy makers and law enforcement officials of the civil liberties issues which may lie hidden in the brambles of telecommunications policy.

"Members of the EFF are speaking at computer and government conferences and meetings throughout the country to raise awareness about the important civil liberties issues.

"We are in the process of forming alliances with other public interest organizations concerned with the development of a digital national information infrastructure.

"The EFF is in the early stages of software design and development of programs for personal computers which provide simplified and enhanced access to network services such as mail and netnews.

"Because our resources are already fully committed to these projects, we are not at this time considering additional grant proposals."

The merits of the EFF are indisputable and we're certainly glad that they're around. But we find it sad that they've redirected their energies away from the hackers because that is one area that is in sore need of outside intervention. There have been an unprecedented number of Secret Service raids this summer with many people coming under investigation simply for having called a bulletin board. And in at least one instance, guns were again pulled on a 14-year-old. This time coming out of the shower. Our point is that someone has to speak out against these actions, and speak *loudly*.

It's also important that what the EFF is actually doing be made clear. Many people are under the mistaken assumption that Craig Neidorf's case was funded by the EFF and that they were largely responsible for getting the case dropped. The EFF itself has not made the facts clear. Mainstream media has given the impression that all hackers are being helped by this organization. The facts are these: The EFF filed two briefs in support of Neidorf, neither of which was successful. They mentioned his case quite a bit in their press releases which helped to get the word out. They were called by someone who had information about the 911 system who was then referred to Neidorf's lawyer. (This is very different from their claims of having *located* an expert witness.) Not one penny has been given to Neidorf by the EFF. At press time, his defense fund stands at $25. And, though helpful, their legal intervention actually drove Neidorf's legal fees far higher than they would have been ordinarily.

So while the EFF's presence is a good thing, we cannot think of them as the solution to the problem. They are but one step. Let's hope for many more.

If you want to get involved with the EFF, we do encourage it. Your participation and input can help to move them in the right direction. Their address is The Electronic Frontier Foundation, Inc., 155 Second Street, Cambridge, MA 02142, phone number (617) 577-1385.

NEGATIVE FEEDBACK

Bringing the Phrack story to the attention of the public was no easy task. But it would have been a lot harder were it not for the very thing that the whole case revolved around: the electronic transfer of text. By utilizing this technology, we were able to reach many thousands of people throughout the world. In so doing, we were able to help the Phrack case become widely known and one of the more talked about subjects in conferences, electronic newsletters, and BBS's. As with anything controversial, not everyone agreed. We thought it would be interesting to print some of the pieces of mail (electronic and paper) from people who DIDN'T like what we were doing. Keep in mind that (as far as we know) these people are not 2600 subscribers and, in all likelihood, have never even seen a copy.

***

"I suppose you've had this discussion an infinite number of times. Nevertheless...:

That old analogy of breaking into somebody's house and rummaging around is quite apt. Nowadays, there are virtually no computers on line that are not protected by password access. Doesn't that put you in the position of a person with knowledge of picking locks? Such knowledge is virtually useless to anybody but a thief; it rarely is of use even to the small community of locksmiths. While I agree that 30 years in the federal slams isn't a just punishment for picking a lock, I suspect that most people found guilty of breaking and entering get lighter sentences, which are probably equally justifiable for computer burglary or whatever criminal label you'd wish to assign to password hacking.

Do hackers do a service? I don't see why. Any mechanical lock can be picked. Probably any electronic scheme can be defeated as well. Yet nobody argues that teenagers should set themselves up as freelance security analysts picking everybody's lock to see if it can be done. If hackers didn't already know they could probably get in, what would be the point?

I see password hacking as a modestly criminal activity somewhere between vandalism, window-peeping, and breaking-and-entering in seriousness, with deliberate destruction or screwing with information as a potentially serious offense depending on the type of information or system screwed with.

Is it necessary to hack passwords in order to learn about computers? Hardly. The country is full of personal computers on which many valuable things may be learned. The cities are full of community colleges, night schools, and vo-tech institutes all clamoring to offer computer courses at reasonable rates. There are even federal assistance programs so the very poor have access to this knowledge. This means that it is unnecessary to commit socially irresponsible acts to obtain an education in computers. The subjects you learn when password hacking are not of use to professional computer people. None of the people I work with have to hack a password, and we are otherwise quite sophisticated.

Privacy is a right held dear in the United States; it's wired into the bill of rights (search and seizure, due process, etc.) and into the common law. You will find that you can never convince people that hacking is harmless simply because it violates people's perceived privacy rights. It is one of the few computer crimes for

which a clear real-world analogy can be made, and which juries understand in a personal way. That's why the balance has begun to tilt toward heavier and heavier sentences for hackers. They haven't heard society telling them to stop yet, so society is raising its voice. When the average hacker gets the same jail term as, say, the average second degree burglary or breaking and entering, and every hacker looks forward to that prospect, I suspect the incidence will taper off and hackers will find different windows to peep into."

There is a common misconception here that hackers are logging into individual's computers, hence the walking through the front door analogy. You'll see it in the letters that follow as well. In actuality, hackers are not interested in violating privacy or stealing things of value, as someone who walks through your front door would be. Hackers are generally explorers who wander into huge organizations wondering just what is going on. They wander using the computers of these huge organizations, computers that often store large amounts of personal data on people without their knowledge. The data can be legally looked at by any of the hundreds or thousands of people with access to this computer. If there's a violation of privacy here, we don't think it's the hackers who are creating it.

This letter raised an interesting point about the "right" way to learn, something many hackers have a real problem with. Learning by the book is okay for people with no imaginations. But most intelligent people will want to explore at some point, figuring things out as they go. Ironically, classrooms and textbooks often discourage people from learning because of their strict limitations. And it's common knowledge that the best programmers and designers are those who are self-taught.

As to the poor having easy access to high technology, this is simply not true. In this country, education is a commodity. And if you don't have the money, you're really out of luck. This is becoming increasingly true for the "middle class" as well.

***

"Using the term 'hacker' to refer to people who break into systems owned by others, steal documents, computer time and network bandwidth, and are 'very careful not to publish anything illegal (credit card numbers, passwords, Sprint codes)' is derogatory and insulting to the broad hacker community, which is working to make the world a better place for everyone."

There has been an ongoing move afoot by older hackers to distance themselves from what they perceive to be the "evil hackers". Their way of doing this has been to refer to all of the "evil hackers" as crackers. While it's a fine tradition to create new labels for people, we think it's a big waste of time here. There is a well-defined line between hacking and criminal activity. Hackers explore without being malicious or seeking a profit. Criminals steal, vandalize, and do nasty things to innocent people. We do not defend people who use other people's credit cards numbers to order huge amounts of merchandise. Why should we? What has that got to do with hacking? While we may find interest in their methods, we would be most turned off by their motivation. There seems to be a general set of values held by hackers of all ages.

***

"I recently read a post to the Usenet (comp.risks) describing recent events related to the crackdown on hackers. While I feel strongly that federal agencies should be scrutinized and held account-

FEEDBACK

able for their activities, the above mentioned post gave me reason for concern that I thought you should be made aware of.

It seemed to me a great irony that the poster was concerned about the invasion of the privacy of BBS operators and users, and yet seemed willing to defend the (albeit non-destructive) invasion of privacy committed by hackers.

I am a graduate student who recognizes the immense importance of inter-network telecommunications. Institutions such as Usenet are becoming vital for the expansion, dissemination, and utilization of creative thought. Any activity which breaches security in such networks, unless by organized design, is destabilizing and disruptive to the productive growth of these networks.

My point is this: I am joe grad student/scientist, one of the (as yet) few that is 'net aware'. I do not want Federal agencies reading my mail, but neither do I want curious hackers reading my mail. (Nor do I want anyone reading company XYZ's private text files. Privacy is privacy.) I agree that the time for lengthy discussion of such matters is past due, but please understand that I have little sympathy for anyone who commits or supports invasion of privacy."

***

"I just finished reading your call to arms, originally published in the Spring 1990 edition. I was royally disgusted by the tone: you defend the actions of computer criminals, for which you misuse and sully the honorable term 'hacker' by applying it to them, and wrap it all in the First Amendment in much the same way as George Bush wraps himself in the American flag.

Blecch.

Whatever the motivations of the cyberpunks (I like Clifford Stoll's term for them), their actions are unacceptable: they are breaking into computers where they're not wanted or normally allowed, and spreading the information around to their buddies. Their actions cause great damage to the trust that networks such as Usenet are built upon. They have caused innocent systems to be shut down because of their actions. In rare cases, they may do actual, physical damage without knowing it. Their excuse that 'the only crime is curiosity' just doesn't cut it.

It is unacceptable for a burglar to break into a house by opening an unlocked door. It should be just as unacceptable for a cyberpunk to break into a system by exploiting a security hole. Do you give burglars the same support you give cyberpunks?

The effort to stamp out cyberpunks and their break-ins is justified, and will have my unqualified support.

I call upon your journal to 1) disavow any effort to enter a computer system without authorization, whatever the reason, and 2) stop misusing the term 'hacker' to describe those who perpetrate such electronic burglary."

We respectfully decline to do either.

***

"I just received the 2600 article on the raid of Steve Jackson Games, which was posted to the GMAST mailing list. It's worrying that the authorities in the US can do this sort of thing - I don't know what the laws on evidence are, but surely there's a case for theft? Taking someone's property without their permission, when they haven't committed a crime?

My only quibble is that the 911 hack-

(continued on page 32)

PRIMOS:

by Violence

Welcome to the final part of my series on the PRIMOS operating system. In this installment I plan on covering Prime's network communications capability and the associated utilities that you will find useful. I will also touch upon those aspects of PRIMOS that I may have overlooked in the previous parts.

Examples appear in italics. Bold italics indicate user input, regular italics indicate computer output.

Primenet

Just like other popular mainframes, Primes too have networking capabilities and support many communications applications. Prime's main communications products are PRIMENET, RJE, and DPTX. I will only be going over PRIMENET in this series, as discourses on RJE and DPTX are beyond the scope of this series. For a good discussion on RJE and DPTX, I refer you to Magic Hassan's excellent article on the subject (appearing in Phrack, Inc., Issue 18).

Available for all models of Prime computers, PRIMENET is Prime's networking software. In a nutshell, PRIMENET is like a Token Ring LAN network. PRIMENET is superior to most Token Ring LAN applications, however. To really be able to visualize how a PRIMENET ring network operates, you need to be familiar with the Token Ring type of LAN (Local Area Network). Token Rings are basically "circles" of computers (referred to as "nodes") that are electronically connected to each other. The individual Prime computers on the PRIMENET ring are responsible for allowing remote users to be able to access them, however. PRIMENET allows for simplified communications between all the netted systems. In the following diagram you will see a sample PRIMENET ring with six Prime computers located on it. Each of the individual nodes may or may not be connected to the telephone network, another PRIMENET ring, or one of the many public data networks (PDN's) like TELENET. Here is an example of the manner in which a PRIMENET ring is set up:

```
PRIME   PRIME
     \_ /
PRIME-(_)-PRIME
     / \
PRIME   PRIME
```

Each node receives information from its neighboring system and transmits it to the node immediately downstream on the ring. In this fashion any node can send information to any other node by sending it through some or all of the others.

As I stated previously, PRIMENET ring networks are superior to most Token Ring LAN applications. But in what ways? Some of the features of a PRIMENET system are listed below:

■ Any terminal on the PRIMENET ring can login to any system on the PRIMENET ring.

■ Processes running at the same time on different systems can communicate interactively.

■ Transparent access to any system in the PRIMENET network without use of any additional commands or protocols.

■ Complete access and protocol

THE FINAL PART

support for packet-switched communications between PRIMENET systems and mainframes located on almost all Public Data Networks (PDN's).

All these features allow you to do things like access disk partitions on system A from system B, rlogin from system A to system B (requiring *only* an account on system B), and so forth. In this installment I will explain the many things that you can (and should) do with a PRIMENET-equipped system.

Checking Out a PRIMENET System

Should you get into a PRIMENET-equipped system, there are a few things that you should do to learn more about the intra-system links and such. In this section I will describe all the procedures that you will need to initiate in order for you to determine said information.

The first thing you should do is to use three of the DSM (Distributed System Management) utilities (remember, I described the DSM in full in Part Two, Winter 1989-90 issue). The three DSM utilities (external commands, really) you should invoke are:

LIST_PRIMENET_LINKS - Lists PRIMENET status

LIST_PRIMENET_NODES - Lists configured PRIMENET nodes

LIST_PRIMENET_PORTS - Lists assigned PRIMENET ports

The information returned to you by these external commands will describe the current PRIMENET setup in detail. You will obtain remote nodenames, PRIMENET addresses, link devices, gateway nodes, configured access, and whether or not the individual nodes require remote passwords for login. Figure A gives a good example of the results obtained from a LIST_PRIMENET_NODES:

This assumes that you issued the LIST_PRIMENET_NODES command from the system VOID. It states that it is on a PRIMENET ring with five other systems (their names can be found in the "Remote node" column). Note the "Primenet address" column. It lists each system's NUA (Network User Address). Notice that three of the listed NUA's are on TELENET and two are on some bizarre network with a DNIC (Data Network Identification Code) of 9999. Well, the host system (VOID) is located on the TELENET PDN (DNIC 3110) and thus, the DSM knows that

FIGURE A

*OK, **list_primenet_nodes***

*** VOID ****

Remote node	*Primenet address*	*Link device*	*Gateway node*	*Configured access*	*Validation required?*
2600HZ	*99994738593624*	*LHC00*		*remote login, RFA*	*no*
THRASH	*3110XXX00254*	*PNC00*		*remote login, RFA*	*yes*
VIOLEN	*3110XXX00245*	*SYNC00*		*remote login, RFA*	*yes*
PSYCHO	*99994734748381*	*SYNC00*		*remote login, RFA*	*no*
SCYTH	*3110XXX00324*	*SYNC00*		*remote login, RFA*	*no*

all 3110 systems are TELENET and displays their TELENET addresses. The other systems (those with the DNIC of 9999) are located on foreign PDN's and the DSM does not understand the addressing scheme (by default it only understands that of the host system) and thusly, displays their PRIMENET addresses.

The "Link device" column tells about the hardware at the individual sites. The host system's device is not displayed, only those other nodes on the ring network. LHC00 is a LAN300 node controller. PNC00 is a PRIMENET node controller (PNC). SYNC00 denotes a synchronous communications line. It's not all that important (unless you are a hardware fanatic, that is).

The "Configured access" and "Validation required?" columns display important information about the linked systems. If you don't see a "remote login" somewhere then you cannot login to the system remotely (you can access it if one of the PRIMENET systems is linked with its disk partitions, however). If you see a "yes" in the "Validation required?" column then some sort of remote password system has been installed and you are going to have a hard time getting in.

As you can see, these DSM commands can be useful when attempting to gain access to other systems on a PRIMENET or LAN300 ring. The rest of this installment will be devoted to utilizing the information gained here to do such.

The PRIMENET RLOGIN Facility

PRIMENET supports remote logins in the same manner that UNIX machines do. If, for example, a PRIMENET ring had six systems on it, four on TELENET and two in the U.K., then you could connect to those systems in the U.K. for free by connecting to one of the 2 U.S. systems and rlogging into one of the U.K. Primes. Using our already defined PRIMENET ring, we'll connect to system PSYCHO from system THRASH.

214 XXX CONNECTED
PRIMENET 22.0.0 THRASH
login system system -on psycho

This will log you in as SYSTEM/SYSTEM on the PSYCHO node (a Prime separate from the THRASH node). This can be *very* useful when you have lost all of your accounts from one node on the PRIMENET ring and do not know the NUA for one of the other ring systems that you still have accounts on.

NETLINK

"NETLINK is a powerful utility and abuse will lead to your account's removal, so be careful in how you use it."

NETLINK is Prime's network utility. All users on a PRIMENET system will have access to this communications utility. NETLINK allows you to connect to:

WITH PRIMENET

■ Other Prime's on the same PRIMENET ring as the system you are on.

■ Any system (UNIX, VAXen, etc.) located on any of the world's networks.

NETLINK is a powerful utility and abuse will lead to your account's removal, so be careful in how you use it. The best thing you can possibly do is use it to connect to and hack on other systems in the PRIMENET ring. If you *must* use the NETLINK utility to call other systems on the world's PDN's, try to call only the systems that accept collect calls.

Now, let me tell you how to get into NETLINK and start doing stuff. At the "OK," prompt (or whatever it has been set to by the LOGIN.CPL file), type:

OK, ***netlink***

If NETLINK is available, then you will see something like this:

[NETLINK Rev. 22.0.0 Copyright (c) 1988, Prime Computer, Inc.]
[Serial #serial_number (company_name)]

After that floats across your screen you will be deposited at the NETLINK prompt, which happens to be "@" (gee, how original). Now, you are all ready to begin NETLINKing.

Time to learn how to connect to a system. Now, there are three types of commands that all do basically the same thing, and that is connect you to a remote system. I'll go over the first two types right now and save the third type for a bit later.

Depending on the status of the system you are trying to call, you will use either C (connect) or NC (connect, no reverse charging). C and NC both do the same thing, but C will make the connection for free (i.e., the people who own this Prime won't get a bill) and NC will make the connection and your net use will be charged. A good comparison is calling NUA's on a PDN. If the NUA is "collectable" (a term I use to describe a system that accepts collect calls meaning no ID required to make the connection), then you will use the C command. Otherwise use the NC command. Almost all international calls will require an NC to connect.

If you simply want to call a system that was listed in the LIST_PRIMENET_NODES list, then do this:

c <nodename>

An example would be:

c thrash

If you wanted to call up a system located on the same PDN as the PRIMENET you are on and the system accepts collect calls, then do this:

c <network address>

An example would be:

c 21398

If you want to call up a system that is located on a PDN other than the PDN your PRIMENET is on, then do this:

c <dnic>:<network address>

An example would be:

C 2624:5890040004

Regardless of what you actually end up typing, you will get one of two things: a connect message or an error message. The connect message for the above example would look like this:

5890040004 Connected

The connect message for when you connect to a Prime on the PRIMENET ring would look like this:

THRASH Connected

Now you simply login (or hack) as you normally would. When you are done, logoff the system as usual. When you logoff, you'll get a message like this:

5890040004 Disconnected

Occasionally you will either type the NUA incorrectly or the system you are calling is down. When that happens you will get an error message that looks like this:

5890040004 Rejecting Clearing code = 0000

Diagnostic code = 0010 (Packet type invalid)

The error message states the network address you tried to call (less the DNIC), the Clearing code, the Diagnostic code, and what the Diagnostic code means in English. Later in this article is a complete list of all Clearing codes and all Diagnostic codes (for reference).

Now, if you want to abort a session prematurely (not recommended unless NETLINK screws up, and it does on occasion), then there are three things you can do:

- Type CONTROL-P
- Issue a BREAK sequence
- Return to TELENET and do a force Disconnect (via the D command)

Those are listed in the order you should try them in. CONTROL-P works most of the time. Doing a BREAK will usually (but not always) close your connection and return you to PRIMOS level. When you do a BREAK, you'll probably see:

UUU@UUu

QUIT.

OK,

Now press RETURN so you can clear out the unwanted CONTROL characters that are in the Prime's command line input buffer. Now, restart NETLINK as usual.

If you are forced to drop to TELENET, then disconnect yourself and re-login. If your process is still online (about 50% of the time), don't worry. It will be logged off due to inactivity in 10 or 15 minutes. If your process got slain then you're in good shape. Now, return to NETLINK as usual.

Ok, now you know how to connect and disconnect from systems. Now it's time for the fun stuff, multipadding and other advanced commands. The escape character for NETLINK is the "@" character (same as with TELENET). Basically, you type:

<cr>@<cr>

to return to NETLINK while online. Doing this will take you back to NETLINK command mode. It will leave the circuit open. To reconnect to the system, type:

continue 1

You will then be reconnected to the system you were on. Now for a slight drawback. If you are using TELENET or any other PDN that uses TELENET's software, then using the NETLINK escape sequence of <cr>@<cr> will take you back to TELENET network command level instead of back to NETLINK command level. There are two ways to correct this problem. The first is to type the following while in NETLINK:

prompt $

This changes the NETLINK '@' prompt to a '$' prompt. Now just type <cr>$<cr> to return to NETLINK. The other way is to utilize TELENET's ITI parameters to turn off the escape sequence. When you connect to the PRIMENET and login, then return to TELENET command level and type these two sequences of parameters exactly as they are shown:

SET? 1:0,2:0,3:0,4:2,5:0,7:8,9:0,10:0,12:0,15:0

SET? 0:0,57:1,63:0,64:4,66:0,71:3

When you return to the "@" prompt, type CONT to return to the Prime. Then just

PART THREE

enter NETLINK as usual. Now when you type <cr>@<cr> you won't return to TELENET as you used to.

Now let's get into multipadding. What exactly is "multipadding" anyway? Well, you probably already know this, but it never hurts to repeat it. Multipadding is what you are doing when you are connected to two or more systems simultaneously. Basically, NETLINK will allow you this capability. Although the NETLINK documentation states that you can only connect to four systems at one time, you can actually connect to more. At any rate, this is how you do it. When you first enter NETLINK (Note: you must set your prompt or the ITI parameters if you plan to do any NETLINKing from a PRIMENET located on TELENET or any other PDN that uses TELENET's software), connect to the first system by typing this:

"Be forewarned that it can be confusing being connected to more than four systems at once."

CALL <nodename> (if it is located on the same PRIMENET ring)

CALL <network address> (if the system is located on the same PDN)

CALL <dnic>:<net address> (if the system is located on a different PDN)

The CALL command will connect you to the system and you will remain in NETLINK command mode. Now, keep CALLing systems until you are done. Be forewarned that it can be confusing being connected to more than four systems at once. Keep in mind that the above CALL examples all assumed that the system that you are CALLing will accept collect calls. If this is not the case, then CALL it like this:

call <whatever> -fcty

The "-FCTY" command stands for facility. When you use the "-FCTY" argument you are basically doing the same thing as you were when you were using the NC connect command. Each CALL that you make opens a circuit. The first circuit you connect to is known as circuit 1, and so forth. So when you are ready to connect to the first system, type:

continue 1

To connect to the second open circuit, type:

continue 2

and so forth. Should you try to connect to a closed circuit you will get the following error message:

Circuit does not exist

To switch between systems return to NETLINK command mode via <cr>@<cr> and then CONTINUE to the appropriate circuit. To close a particular circuit, type:

d #

where # is the actual circuit number. An example would be D 1 or D 3. There must be a space between the D and the circuit number. To disconnect from all open circuits you can type:

d all

That's pretty much all there is to multipadding. It's nothing special, and not really that useful, but it can be interesting to connect to two or three chat systems and switch between them, or hang on a chat and leave to hack a system while remaining on the chat, etc. There are lots of interesting things you can do. When you are done

(continued on page 34)

AN INTRODUCTION

by The Plague

Introduction

The COCOT, more precisely, the Customer Owned Coin Operated Telephone: good or evil? To the COCOT owner it's a godsend, a virtual legal slot machine for leeching the public, freeing the owner from the monopolies of the phone company. To the public it's a nightmare, a money-stealing machine providing poor service and insanely high rates, a virtual hotel-style phone in the guise of an innocent looking payphone.

To the telephone enthusiast, a COCOT is something else entirely. A treasure trove of tasty parts perhaps, including microprocessors, coin identification mechanisms, tone dialers, tone and call progress detectors, a modem for remote connections, speech synthesis and recognition equipment, magnetic strip readers for credit cards, and other parts to be explored and tinkered with. For other phreaks, the COCOT represents an unrestricted phone line which can be used for exploration of the phone system. Still, for others, COCOTs can represent a storage house of long distance access codes and procedures. Others may see the neighborhood COCOT as a bunch of imprisoned coins and a future wall phone for their room. Many more treasures are to be found in a single COCOT, as you shall soon see.

COCOT Basics

To those of you unfamiliar with the COCOT, let me quickly fill you in on the basics. Firstly, most, if not all, COCOTs operate on regular business or residential (depending on the greed of the owner) phone lines. There are exceptions to this rule in a few major cities where private-payphone lines are available directly from the local phone company; these allow the use of regular operators who are aware of the status of the line as being COCOT based. However, few, if any, COCOTs use this type of line, even when it is available.

Almost all COCOTs are microprocessor-based devices, thereby making them smarter than your average phone company payphone. A major function of the COCOT is to independently collect coins in return for time during a call. While the real payphone uses the ACTS system on a remote phone company computer for coin request and collection functions, the COCOT performs these functions locally in its small computer. Naturally, red boxes do not work with COCOTs. However, since their coin detection mechanisms are not as advanced as those in real payphones, it is much easier to trick them with slugs.

The dialtone you hear when you pick up the handset to a COCOT is usually not the actual dialtone, but a synthesized one (more on the dialtone later). As you press the numbers on the keypad, the COCOT stores each number in memory. The keypad may or may not be DTMF, depending on the phone. Most COCOTs do not allow for incoming calls, since their primary purpose is to generate revenue, and incoming calls simply waste time which could be used by paying COCOT customers (from the owner's point of view). If you obtain a number to a COCOT, it will usually pick up after several rings in remote mode (more on that later).

After the COCOT has enough digits to dial your call, it will ask for the amount of money to deposit on an LCD screen or in a synthesized voice, unless you have placed the call collect or used a calling card, or if the call is toll-free. It will then obtain an actual dialtone from the phone line, and dial your call through whichever method it is designed to use. During this time it may or may not mute out the handset earpiece and/or the mouthpiece. For local calls, it will usually dial the call directly, but for long distance, calling card, and collect calls, it will usually use an independent hotel-style phone company or PBX. This is done so that you (or the called party in a collect call situation) will be charged up the wazoo for your call. If it detects a busy, re-order, or other progress tone other than a ring, it will refund your money and not charge you for the call, in theory. In actuality a lot of COCOTs will rip you off and charge you anyway, hence their reputation. Unless the call was placed collect or with a calling card or toll-free, the phone will periodically ask you to deposit money. Since the small and sleazy long distance companies used by most COCOTS are chosen on the basis of rates, rather than quality, you can be sure that most calls placed on COCOTs have an extremely large amount of static and bizarre

TO COCOTS

echoing effects.

Identifying COCOTs

A lot of people (non-phreaks) seem to have trouble telling COCOTs apart from phone company payphones. I can spot a COCOT a hundred yards away, but to the average person, it's pretty tough because they are made to look so much like the real thing. Actually, it's quite simple. Just look for your RBOC's (New York Telephone, Southwestern Bell, etc.) name and logo on the phone to be sure it's the real thing. Ninety-nine times out of a hundred, it's a real payphone. The rare exceptions occur when it's a COCOT made and/or owned by your local phone company (in which case, not to worry, these won't rip you off as badly as the sleazy small-company made phones), or when it is in fact a sleazy small-company made phone, disguised by its owner, through the theft and re-application of actual payphone signs and markings, to be indistinguishable from the real thing. The latter case is illegal in most parts of the country, but it does happen. Nonetheless, a phreak will know a COCOT as soon as he dials a number, regardless of the outer appearance. The absence of the true ACTS always means you're using a COCOT.

"To the public it's a nightmare, a money-stealing machine providing poor service and insanely high rates."

COCOT Varieties

Let us discuss the various varieties of COCOTs. To be frank, there are actually too many different COCOT devices to discuss them individually, and their similarity in appearance to one another makes for difficult identification even to the advanced COCOT (ab)user. They range from simple Western Electric look-a-likes, to more advanced varieties which may include LCD or CRT displays, credit card readers, and voice-recognition dialing. The range is very wide with perhaps 1000 different phones in between.

In reality, you should approach each new COCOT with no pre-dispositions, and no expectations. Experiment with it, play around with it, see what kind of COCOT security measures (more on that later) it implements, attempt to gain an unrestricted dialtone, see how well the beast is fastened to its place of inhabitance, attempt to decipher its long distance access methods, and so on. In general, just play with it.

Getting the Dialtone

I started research for this article with the intent of explaining which techniques for obtaining actual unrestricted dialtones work with what phones. In my exploration, I have learned many tricks for achieving this, but have also found that there are too many differing COCOTs out there, and devoting an article to defeating a dozen or so brands that can be found in the NYC area would be a waste of my time and yours. Instead, I have focused on general techniques and methods that can be applied to any new, unknown, or future variety of COCOT.

I have decided to break this down into the various COCOT security measures used by COCOTs and how to defeat each one. In actuality, each COCOT seldom uses more than one of these COCOT security measures. When a single COCOT security (anti-phreaking) measure is used, it is quite easy for the phone phreak to obtain a dialtone. In more secure COCOTs, you should experiment with various combinations of these techniques, and attempt to come up with some techniques of your own.

To begin with, the most basic attempt to get a real dialtone requires you to dial a toll-free or 1-800 number, wait for them to hang up, and wait for the real dialtone to come back. At which time, you would dial your free call on an unrestricted line, or better yet, dial 0 for an actual operator and have her place the call for you. The following are methods used by COCOTs in order

to stop you from doing this. Like I said, it is rare for any specific COCOT to implement more than one of these.

COCOT Security Measures and How to Defeat Them

1) Locking Out The Keypad - If the keypad is DTMF, the COCOT will lock it out after your original call is placed. This can be defeated with the use of a portable DTMF dialer provided that other measures are not in place to prevent this (muting, DTMF detection, and automatic reset).

2) The Use of a Non-DTMF Keypad - Here, again, the purpose is the same, to prevent further dialing after the call is completed. Again, this can be defeated with a portable dialer, provided other measures are not in place. Most COCOTs dial-out using DTMF anyway, and hence DTMF dialing should be enabled for that line.

3) DTMF Detection & Automatic Reset - Here, a different approach is taken to prevent unauthorized dialing. The phone will reset (hang up and give you back the fake dialtone) when it detects DTMF tones on the line after the COCOT dials your call. Most COCOTs do not implement this measure because it interferes with legitimate applications (beeper calls, VMB calls, etc.). To defeat this measure, modify your portable dialer to use shorter tones (less than 50ms). Since the central office (CO) can usually detect very short tones, whereas the COCOT may be sensitive only to longer tones, you should be able to dial out. Another way to defeat this is to mask your tones in synthetic static generated by blowing a "shhhhhhh" sound into the mouthpiece as you dial the first digit on the unrestricted dialtone. This should throw off most DTMF detection circuits used in COCOTs, and tones should be received quite fine at the CO because their circuits are more advanced and provide greater sensitivity and/or noise suppression.

4) Dialtone Detection & Automatic Reset - This measure is similar to the above measure, except resetting will take place if a dialtone (the unrestricted dialtone) is detected by the COCOT during the call. Since most COCOTs do not use the "hang-up pulse" from the CO to detect the other party hanging up, they rely heavily on detecting the dialtone that comes afterwards, in order to detect when the other party hung up. This is a clever measure that is easily defeated by blowing a "shhhhhhh" sound (synthetic static) into the mouthpiece during the time at which you expect the real dialtone to come back. As you keep "shhhh"ing, you will hear the dialtone come back, then dial the 1st digit (usually a 1), the dialtone will be gone, and you dial the rest of the number. If the keypad is locked out, use your portable dialer.

5) Number Restriction - Most COCOTs

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

Photo Salvation
Ken Copel

Design
Zelda and the Right Thumb

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Log Lady, The Plague, The Q, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Mr. Upsetter, Violence, Dr. Williams, and the faithful anonymous bunch.

Remote Observations: Geo. C. Tilyou

will restrict the user from dialing certain numbers, area codes, and exchanges. Usually these include 0 for obvious reasons, 976 and 1-900 type numbers, ANAC (number identification), and others. On rare occasions, COCOTs will restrict you from dialing 1-800 numbers. Although this is illegal in most parts, it is done nonetheless, because most COCOT owners don't like people using their phone without paying them. In practice this brings in more revenue, because the phone is available to more paying users. Your best bet here is to call any toll-free number that the phone will accept instead of the 800 number. These may include 411, 911, 611, 211 or the repair or customer service number for the company that handles that COCOT (this is usually toll-free and is printed somewhere on the phone).

6) Muting The Mouthpiece - This is not really a measure in itself, but is sometimes used in combination with other measures to prevent dialing out. Muting is usually done when the COCOT itself is dialing out, which prevents you from grabbing the dialtone before it does. This is a rather lame and futile technique since we typically obtain the unrestricted dialtone after the call is completed. Thus, there is no need to defeat this. I suppose the designers of the COCOT were really paranoid about security during the start of the call, but completely ignored dialtone penetration attempts after the call was dialed and connected. Just goes to show you what happens with those guys who wear pocket protectors and graduate with a 4.0 average. In theory their designs are perfect; in reality they never match up to the abuse which we subject them to.

7) Other Measures - Although I have discussed all measures currently known to me, in defeating new measures or measures not discussed here my best advice would be to use a combination of techniques mentioned above to obtain an unrestricted dialtone or a "real operator" (local, AT&T, or any operator that can complete a call for you and thinks you are calling from a regular line, not a COCOT).

Secret Numbers

Actually, there's not much to say about secret numbers. Most COCOTs have secret numbers that the owner can punch into the COCOT keypad, in order to activate administrative functions or menus, locally. These functions provide information regarding the status of the unit, the money in the coin box, the owner's approximate phone bill, and various diagnostic and test functions. They also allow a certain amount of reprogramming, usually limited to changing rates and restricted numbers. For more information about these, I would suggest obtaining the engineering, design, or owner's manuals for the unit. Since engineering and design manuals are closely guarded company secrets, mostly to prevent the competition from cloning, it would be very difficult to obtain them. Owner's manuals can be obtained rather easily with a minimal amount of social engineering, but they are sadly lacking in information, and primarily written for the average COCOT owner.

Remote Connections

Remote connections provide the same functions as described in the previous section, except they can be accessed from remote, by calling the COCOT. Remote connections are usually reserved for authorized users (the company in charge of maintaining the proper operation of the COCOT). Thus, the COCOT can be diagnosed from remote, even before a person is sent down to repair it.

A typical COCOT will pick up in remote mode after someone calls it and lets it ring for a while (between 4 and 10 rings usually). At that time it will communicate with the remote site using whatever method it was designed to use. This is usually a 300 baud modem, or a DTMF/synthesized voice connection. An access code is usually required, which may be a 3 or 4 digit number in the DTMF connection, or anything for a password in the modem connection.

(continued on page 42)

Hunting for Wiretaps

Dear 2600:

This is in response to WH's letter from upstate New York. I want to clue you in on the shortcomings of the phone company in looking for wiretaps.

When you first tell the phone company, they will run a computer check to look for something in series circuit with their phone lines. They will only look for series circuits because that is the only way *they* wiretap. When they don't find it they probably will call you back and say they didn't find it and you're paranoid.

If you insist that they check the phone lines again, they will probably send someone out to your neighborhood to check the ends of the cables. They will put a multimeter up to the ends of the cables to look for either a voltage drop, current change, or an impedance across the lines. Here again they are looking for a series circuit device.

The problem is that the phone company doesn't believe in parallel circuits or any other types of circuits. The parallel circuit must have infinite input impedance, possibly an op-amp.

When they don't find the wiretap the second time, they will probably give you the routine, "Why would anyone single you out to wiretap your phone?" Then words to the effect that you're paranoid. The bottom line is that the telephone company is technically incompetent.

If you really want to check your phone lines, do it yourself. There are only 12 volts on the line, very little current. Put your hand on the cable and follow it out. When you come to something on the cable, open the cover and see what's in there. You may have to climb up the three or four telephone poles near the telephone that is being bugged.

The best solution is to have the phone disconnected and not use it at all. Use pay phones, different ones at different locations.

Question: How does someone wiretap into US Sprint's fiber optic network? It's been done to me.

San Francisco

Don't climb any telephone poles unless you know what you're looking for and can tell the difference between phone wires and electric wires. Sprint readers: any clues?

Comments

Dear 2600:

As a 58-year-old hacker I find more *solid* info in *2600* than *Byte, Compute,* and *Computer Shopper* combined.

At present it's legal for "Big Brother" to listen in on wireless phones without a judge's permission yet I can't use a radar detector in some states. What happened to the Constitution and the Bill of Rights?

Fred
Wilmington, Delaware

That yellow paper fades with age....

Dear 2600:

I recently received my first issue of *2600.* I am very pleased with the content of the magazine, but not the condition. The copy I received was in extremely poor condition. The middle four pages were missing, and all the pages from the center through the back cover were ripped.

I filed a complaint form with the U.S.P.S. but they have not replied. Is there anything that you can do?

Secondly, can you send the magazine first class? Those magazines that I receive by first class seem to survive the post office in much better condition than those sent otherwise.

Milwaukee

We send the magazine out second class which is exactly the same as first class except it's a whole lot cheaper. (It's a rate for magazines.) The best thing you can do is file a complaint with the post office. We'll send you a replacement copy.

On Government Raids

Dear 2600:

Regarding your recent attempts to publicize the government raids of com-

puter bulletin boards: This is a particularly silly-looking situation from my perspective. I work in the telecommunications industry, for a voice response service bureau partially owned by MCI. We deal with tariffs and communication law all the time. Would the established telecommunications industry ever stand for being held responsible for illegal activities conducted in phone calls being carried over their networks? Never. It's stupid. The Internet and UUCP are as much common carriers as AT&T and Sprint — why should they be treated differently?

But you know all this. I need not pontificate now; I'll save it for my legislators. Anyway, if you know of any legislation in progress that pertains to this freedom of information topic, please let me know.

STM

Dear 2600:

Just sent you a paper copy of a fascinating book from the US NTIA/GPO/telecom office called *Emergency Medical Services Communications System Technical Planning Guide.*

Slightly dated, but most of the info is still in use as described (main difference is that some frequencies have been changed and there's now some true digital communications).

Anyway, the reason for sending you the book, aside from general info, is that there is an extensive discussion of how 911 systems operate. Seems that if you can get a book like this for $15 (out of print now, but I have numerous copies), it seems a bit ludicrous to claim the "911 document" is worth tens of thousands.

DB

It was because of the efforts of people such as yourselves that the case against Neidorf and Phrack was eventually dropped. Yet another example of how knowledge shared is a good thing. Thanks for the support.

For the Record

Dear 2600:

It's ANAC (Automatic Number AnnounCement), not ANI (Automatic Number Identification)!

The Acronym King

Questions

Dear 2600:

Sure it's true that red boxing is safe, but surely someone has been caught. If you have any news on how red boxing is investigated, I'm sure it would be very interesting reading.

Also, I'm in a situation that I bet a lot of other subscribers are in too. I have a partial year of 2600 and would like to purchase back issues. However, I just can't bring myself to pay $25 for what would only be a half year of new information. Anything I can do?

Simpson

If you have a partial year of 2600 for 1988 to the present, you can buy individual issues for $6.25 each ($7.50 overseas). Anything before that is only sold by year.

Speaking of red boxes, a couple of readers proved us wrong in one of our replies to letters in the last issue. They came up with plans to change a Radio Shack touch tone dialer into a red box! We never said it was impossible; we simply wondered why anyone would bother to do this. We hope to show our readers how and why in the very near future.

Dear 2600:

Pray tell me, if you please, which of your back issues would have the ringback number for my telephone number in the 404 area code?

BM

We looked, and either we missed it or we never gave it out. Ringback codes are generally too area specific to be given out here. Every exchange can be different. But the best way to find such codes, as well as ANI (ANAC to perfectionists), hidden exchanges, and other fun things is to explore every possible exchange in your area code. Our August

we welcome letters

1984 issue has a worksheet you can use to accomplish this.

At press time, a brand new 800 ANI demonstration was still working. By calling 800-666-6258, you can actually have your number read back to you (instantly if you hit a touch tone when it picks up). Yes, 800 numbers can tell who's calling them; we've been telling you that for some time. Now you can see it for yourself. But there are also ways to defeat the system. One is by asking the operator to complete your call to the 800 number. ANI gets the area code right, but replaces the phone number with all 5's. Some people have reported getting all 0's from remote locations. We want to hear what other experiments yield. We hope this service stays around for awhile, as it's invaluable in finding out COCOT numbers, extender and diverter numbers, PBX outdials, etc.

Dear 2600:

Do you know the addresses of any of the following magazines? I've been looking for them (along with *2600*'s which I found by accident in an issue of the *Village Voice*) for some time now. They are: *Reality Hackers, New Realities, W.O.R.M., Cyberpunk International, Mondo 2000, Street Magazine* (published in Boston).

JI
Iceland

W.O.R.M. is no longer published. However, its editor is working on a new publication which should be out in the near future. We'll keep you posted. Reality Hackers is the old name for Mondo 2000. Their address is PO Box 10171, Berkeley, CA 94709. Street Magazine is at PO Box 441019, Somerville, MA 02144. As for the others, we'll have to ask our readers for help.

Dear 2600:

I am very interested in telephone surveillance and counter-surveillance as well as cellular phones. If you have any back issues on these topics I would like to buy them.

Also, I recently dialed a CN/A operator and she asked me for my ID number, which I obviously didn't have. What do I do?

Jeff

We're looking for a few good articles on tapping in the nineties. We haven't really covered surveillance in itself. As far as "logging in" to the CN/A operator, we suggest you find out one bit of information at a time: format, what kind of companies have codes, etc. It's called "people hacking" and you don't even need a computer.

Dear 2600:

I just picked up a copy of the Autumn 1989 issue of *2600* in a secluded bookstore in The Russian River area of California. It contains a list of carrier access codes but when I dial the code followed by 700-555-4141 I get the message "It is not necessary to dial '1' with this number" and then a busy signal. What am I doing wrong?

Also, how can I get more information about using my computer to access BBS systems without paying exorbitant long distance charges (I currently use AT&T and pay them $200-$300 per month to call a board in Youngstown, Ohio.)

Do you still have a BBS service and could you explain the difference between blue boxing and red boxing?

Guerneville, CA

It sounds like you might be in a non-Bell area. Independent local companies (such as GTE/Contel) sometimes don't have equal access and provide horrible service. You're probably confusing the hell out of your switch by dialing something it's never heard of before. Hence the weird recording.

Re BBS service: You might want to check out PC Pursuit, the service run by Sprint that allows you 30 hours of connect time (almost) anywhere in the country for $30 a month. You should make sure that you can connect to Telenet for the price of a local call and that the boards you call are reachable on PC Pursuit. Call 800-TELENET and ask all the questions you want.

We don't have any BBS's nor can we recommend any as everyone seems to be in a state of paranoia. We can't emphasize

enough the importance of using bulletin boards to communicate freely, openly, and anonymously (when necessary). If you have the capability of running a board, we highly recommend it.

Finally, blue boxing hardly works at all in the U.S. It involves seizing long distance trunks with a 2600 hertz tone and then routing calls for free using MF tones. A blue box basically gave you the power of an operator. What a red box does is play five beeps which tell unsophisticated old-fashioned Bell-operated payphones that you've dropped in a quarter. This still works all over the country.

Protection From Eavesdroppers

Dear 2600:

The article in the Spring 1990 issue on marine telephone eavesdropping brought back memories of some 10-20 years ago when I worked as a part time marine electronics tech. At that time most pleasure boat radios operated in the 2-3 mHz AM band. VHF and SSB were just beginning during this time. The coast radio telephone stations at that time (and most likely still) consisted of three parts, all connected by wireline or microwave links.

First, there were several receiver sites scattered around the service area.

Next, there was one powerful transmitter located at a central site.

Last, there was a control point where the operator(s) sat.

Whichever receiver was getting the strongest signal for the moment locked out the others and was heard by the operator. The operator could read out the signal strengths of the various receivers, and they usually didn't mind going down the whole list if you called them as "radio repair" during a slow period. This also told you the locations of the receivers, because she (male operators were *very* rare then) would give the location and the signal strength for each one. Another control she had was a "cover tone" switch. When on, the shore transmitter, instead of rebroadcasting the ship station, would just go beeeeeeep pause beeeeeeep pause...whenever you (on the boat) had your mike button pressed. (Ship to shore telephone service is half duplex instead of full duplex as is landline and cellular service. Half duplex means that only one side can talk at once. The boat station controls the direction that is active by pressing and releasing the mike button. The person on the boat can interrupt the person on land, but not vice versa.) I made it a point for myself and to my customers to always ask the operator to "stop repeating me" (i.e., turn on the cover tone) when I gave a credit card number or any such information I didn't want broadcast over the entire NYC-NNJ-LI area. With rare exceptions, they did so without complaint. I would suggest that this is still a good idea.

Caution: This won't make you completely immune to eavesdropping, but it will greatly reduce the likelihood. An eavesdropper would have to hear the relatively weak signal from the boat instead of the much stronger shore station signal.

RG

We're told that as a result of our article in the last issue, the entire policy of giving calling cards out over the marine band has been stopped. Some people are angry with us because this avenue of free calling has been turned off to them. But counter that with the fact that certain companies had to fall over themselves changing a non-existent security policy before the whole world found out about it. Plus the fact that yet again we've proven how customer security really isn't all that high on their priority list. It would have had to have been changed at some point, anyway. Better that it go out with a bang than a fizzle.

2600 Compromising Ideals?

Dear 2600:

Through the years, *2600* has received from its readers much praise for its efforts to make available a certain amount of information to the computer/ telecommunications hobbyist that can be found nowhere else. But I think that *2600*'s actions of late are nothing less than reprehensible and are detrimental to the very same community it tries so hard to defend. It is my hope that you will print this letter in full, as lengthy as it may be, to allow the members of the hacker community outside of the New York City area to understand the recent turn of events you have alluded to on pages 38-39 of the Spring 1990 issue.

"We do not believe in cover-ups. By not printing that bit of ugliness, we would have been doing just that." - *2600 Magazine*, Autumn 1988, page 46.

This brings me to the main thrust of my letter: Lately, in the New York City area, hackers have been receiving quite a bit of media attention, probably more than ever before. This has ranged from newspaper and magazine articles to local NBC news coverage of the UAPC hacking ordeal. In each instance, *2600 Magazine* has been prominently mentioned, and your editor has appeared in both televised and printed interviews. Due to these appearances, it is becoming readily apparent to the society outside of our "subculture" that *2600 Magazine* is a "spokesperson" for the hacker community.

I have nothing against that. In fact, the hacker community needs a unifying force or even a tangible home base where hackers of different backgrounds and computers can interface. The presence of *2600* itself, as a public voice for hackers, may also prove to be a medium through which we can help expose inequities in the system itself, in this world of Secret Service confiscations and arrests, biased trials, and unjust sentences.

What I am protesting, however, is the image *2600 Magazine* is projecting of the "American Hacker" to the outside world. Since its beginning, *2600* has coveted its beloved disclaimer of how the hacker is born out of the desire for intellectual stimulation, which can be satiated via the use of a computer and the exploration of it and others with it. *2600* feels this is how the world should view us. I quote from Spring 1988, page 8: "...hacking involves so much more than electronic bandits. It's a symbol of our times and one of the hopes of the future." This may be a rosy-eyed, naive view, but it is, however, accurate.

But lately, *2600 Magazine* has drifted from this ideology, and the hacker is gaining a reputation as a criminal with destructive intent, as the editors and writers of this magazine are getting caught up in the sensationalism of it all. The pictures of several members of the close-knit group of friends (I will call the "*2600* Gang") appeared on the front cover of the *Village Voice* the week of July 24, 1990, and Eric Corley himself has appeared on both an NBC prime-time television newscast and in the cover story of *Newsday Magazine*, July 8, 1990, page 12. This simply supports my argument that *2600 Magazine* is compromising the security of its subscribers, as well as that of fellow members of the hacking community, to gain a spot in the limelight.

Perhaps it is *2600*'s belief that society should be made aware of our "habits", to "show how the machine really works". Does this include the public announcement of the "Flare Gun Assaults" that *2600 Magazine* has conducted against several telco instal-

lations? Or does it include televised admissions that the *2600* staff has penetrated the New York City Board of Education's computer system? Does it also include concessions that close affiliates of *2600 Magazine* are reprogramming ESS switches?

Do you realize the repercussions of your bragging and arrogance? *2600 Magazine* is the *only* place where such material can or should be discussed, where it will gain worldwide acceptance. The outside world will condemn *2600 Magazine* for its actions and all hackers along with it. If the "spokesperson" of the hacker community itself is tied to such activities, then hackers will be depicted to the world as perpetrators of crimes far worse than those mentioned above and will be considered detrimental and a threat to society as a whole.

Your magazine speaks of ignorance of "the system" and the resultant fear of it. In fact, *2600 Magazine* was created in an effort to enlighten people and dispel this fear. But of late, *2600*'s activities and their glorification by the media, are generating a fear of hackers themselves, which is already developing into a hatred. In the public's eye, the hacker has degenerated from the forgotten War Games character, an inquisitive and smarter-than-average teenager with a gift for computers, to a malicious cyberpunk that is a threat to society and cannot be trusted in it. This computer whiz kid that was once greatly desired in the work force for his knowledge and ingenuity is now banned from employment in the computer science field as a security threat, and is being viewed as a criminal and the keyboard his weapon.

I am not claiming innocence. Far from it. No "true" hacker can. But certainly your recent activities and efforts to gain some fame are sacrificing everything for us, since you are being viewed as the representative of our entire community. When *2600 Magazine* was founded in 1984, I don't think this was what you set out to achieve.

The recent trend of events at your monthly meetings is further evidence of this. The meetings have deteriorated from an informative assemblage of hackers to a chaotic throng of teenagers who are being viewed by the media and authorities as a menace. Within this mob is hidden the "*2600* Gang", a very elitist group of close-knit friends who associate with Eric Corley and refuse to share information or communicate with anyone outside of it. This is just another example of the hypocrisy of this magazine and its staff, which has thus far claimed to encourage the free exchange of information to promote awareness.

In light of this, I urge the staff of *2600 Magazine* to re-evaluate its ideals and actions and to come to grips with the responsibility it has to take on if it wishes to deal with the media in any way. At this time, it might be best to discontinue all media contact and relocate the *2600* meeting place to a more discreet location. If anyone wishes to take on the media individually, he should not implicate *2600 Magazine*, as it will simply associate the magazine with illicit activities, which will result in further arrests, confiscations, and eventually, the closing down of *2600 Magazine* as well as the compromise of its subscribers' list in a big FBI coverup a la *TAP Magazine*. I know that the majority of the "*2600* Gang" who are less mature than the editors will dismiss this letter as a sign of paranoia and foolishness, but it is not. This is very serious.

Disgusted Hacker

It's interesting that you accuse us of "refus[ing] to share information or communicate with anyone outside of [our group]." Yet your solution is to "discontinue all media contact and relocate the 2600 meeting place to a more discreet

location", which no doubt would have less "chaotic teenagers". Sounds like you just want more of a grip on the situation.

Our meetings are chaotic, no question there. We see them as a parallel to what hacking is all about. We trade information, talk with lots of people, make a bit of noise, and move forward without any formal agenda. We're careful not to cause damage, but sometimes people get offended. It's not for everyone.

In such a community, there can be no one unifying voice that speaks for everyone. And 2600 does not speak for all hackers. Nevertheless the media has called upon us to participate in and help investigate particular hacker stories. This has resulted in, despite your claims, some of the best hacker press in years. We fail to see how this could compromise the security of our readers or of anybody else for that matter. Recent articles in The New York Times, The Village Voice, and Harpers have shown hackers in a more realistic light (the Voice piece in particular being one of the best articles ever to have appeared on hacking). A National Public Radio program in August pitted hackers against Arizona prosecutor Gail Thackeray in a lively debate. Even television is starting to show potential, but that's going to take some doing. Sure, there's still a lot of mudslinging going on. But most of this is the result of events, such as the massive raids by the authorities over the past few months. Were it not for the better stories that could not have been written without our participation, the American public would have gotten only one side. Is this what you want?

You refer to another article that accuses hackers of reprogramming switches and shooting flare guns. But you're the only one who says 2600 is in any way connected with these alleged incidents. Why? You're also the only one who says 2600 broke into the UAPC system (Grade "A" Hacking, Autumn 1989 issue). It was very clear in every account we saw that the UAPC information was given to us and that we turned it over to the media. Since you're obviously capable of getting our quotes from past issues of 2600 right, why can't you get the basic facts right on such important stories? It reminds us of a recent case where a hacker from New York was reported to have had access to telephone switches. The New York Post took that to mean that he opened manhole covers in the street to access the phone lines — and that's what they printed. Needless to say, we had nothing to do with THAT story.

We're not saying that your concerns are not valid. The image of the hacker is constantly being tarnished by people who either don't understand or who want to see hackers cast in a bad light. But your facts just don't hold up. Our public stands have had an effect. Journalists must prove their integrity before we give them a good story. And when a good story comes out, the average reader has the chance to see hackers as we see ourselves. With that comes the hope that they will understand.

An Unusual Request

Dear 2600:

I would like to ask your readers to help me make a plane crash. Specifically, I need to know how a multi-millionaire media magnate could willfully cause a jetliner to crash on approach to a major New York airport *via computer dial-up.*

My name is Rick Saiffer, and that's part of the story for a screenplay I'm writing. I entreat *2600* readers to help make it realistic, creative, and especially devious. (In case you're wondering, the hero of this movie is a hacker who will eventually *discover* that the millionaire caused the crash, via sloppy

middle island, ny 11953

hacking mistakes *he* made while *engineering* this crash!) I want the crash to be big: two 747's colliding in mid-flight over the Grand Central Parkway at rush hour would be delightful.

I imagine that this hacking would take place pre-flight, but I'm open to suggestions. Remember, our villain has unlimited money and power, so have fun: money is no object!

Please send responses to: Plane Crash, c/o 2600, P.O. Box 99, Middle Island, NY 11953. Include some form of return address if you wish; I would like to contact the best respondents directly.

Free Phone Calls

Dear 2600:

In the past you have printed letters telling tales of woe about flawed college telephone systems. I recently discovered an interesting flaw in the telephone system at my university. All students living in the dorms must dial "8" first to dial out on local and long distance calls. However, if one merely dials "7" instead of "8" before any long distance call, the call doesn't show up on your bill. Now those are the kind of flaws that I like.

Mr. Upsetter

They're also the kind that don't last very long.

Dear 2600:

I learned of a trick that might be of interest to you. To get someone else to pay for your long distance calls when you're in a payphone, grab the phone book. Dial 0 and the number you want to reach. Then tell the operator, when she comes on, that you want to bill this call to another phone. When they ask if someone is home to verify it, say, "I think so." For selection of the number, there are several methods to use.

(a) The number of someone you know (and presumably hate), using the name of one of their loved ones who might ask them to take the charge.

(b) A number at random from the phone book, using the name of the person who is listed for the number.

(c) A number at random from the phone book, using a bland name like Joe, John, Frank, Bill, Sam, et cetera. (This works more effectively on phones designated "Children's Phone" and phones in rich neighborhoods.)

(d) A person's office. After hours, many people have answering services covering their calls, and every once in a while they might accept charges if you use the name of the person who employs the service.

Warning: Be prepared to hang up, especially on (b) and (c). The odds of actually succeeding are low, but not as low as you might think. (The person who told me this trick pulled it off the first time he tried it, and has done it twice since. Most of the time, nobody's home.) Also, if you're doing this from a payphone, it's practically impossible to get yourself caught unless you're trying.

There is the difficulty of running into the same operator twice or thrice, but this can be avoided by having two or three people running shifts calling four or five times in a row and then passing it along to the next person. It's easier for the caller to recognize the operator's voice than vice versa, especially since they speak first, but be prepared to pass the phone to another person quickly.

(In case you're wondering, my friend is a bored dorm student who gets desperate to talk to his girlfriend who lives several hundred miles away.)

Birmingham

We'll be honest. Your methods are as old as the hills. Apart from that, simply billing calls to another person really doesn't have all that much to do with hacking. But continuing to figure out ways around the system does. We hope you know the difference.

(continued from page 13)

ers are not innocent. Yes, they may well be innocent of computer vandalism, forgery, etc. (the only consistent truth about newspapers is that they couldn't get facts straight to save their lives) but they have still entered a system and looked at a private document (assuming I understood your article correctly - apologies if I'm wrong). People should have a right to privacy, whether those people are ordinary users, hackers, or large companies, and it should not be abused by either hackers or the authorities. Consider the non-computer analogy: if someone broke into my house and started going through my things, I would be severely unhappy with them - and I would not appreciate a suggestion that they had a right to do so because they happened to have a key that fit my door!"

***

"What does the entire 911/Steve Jackson Games escapade tell us? Well, it's not all that new that the government (like most such things) requires careful watching, and I'm not too happy about how the last I'd heard, an agent had told SJ Games they wouldn't get all of their hardware back, even though no charges had been filed. (Can you say legalized thievery boys and girls? I knew you could.)

But the main thing that moves me to write this missive is the indication from the published article that the authors, and thus quite likely also the party responsible for copying that document and circulating it still do not quite understand what the individual responsible did. Accordingly, and in the hopes that if this circulates widely enough he or she will see it, the following message:

OK - all you did was get into Bell South's computer system (mostly proving that their security sucks rocks) to prove what a hotshot hacker you were, then made a copy of something harmless to prove it. Sheer innocence; nothing to get upset about, right?

Bullshit, my friend. Want to know what you did wrong? Well, for starters, you scared the U.S. government and pointed it in the direction of computer hobbyists. There are enough control freaks in the government casting wary eyes on free enterprises like BBS systems without you having to give them ammunition like that. Bad move, friend, bad move. You see, the fact that you didn't damage anything, and only took a file that would do no harm to Bell South *or* the 911 system if it were spread all over the country is beside the point. What really counts is what you *could* have done. You know that you only took one file; Bell South only knows that one file from their system turned up all over the place. What else might have been taken from the same system, without their happening to see it? You know that you didn't damage their system (you *think* that you didn't damage their system); all Bell South knows is that somebody got into the system to swipe that file, and could have done any number of much nastier things. Result - the entire computer you took that file from and its contents are compromised, and possibly anything else that was connected with that computer (we know it can be dialed into from another computer - that's how you got on, after all!) is also compromised. And all of it has now got to be checked. Even if it's just a batch of text files never used on the 911 system itself, they all have to be investigated for modifications or deletions. Heck - just bringing it down and reloading from backup from before you got in (if they *know* when you got in) even if no new

FEEDBACK

things were added since would take a lot of time. If this is the sort of thing that $79,449 referred to I think they were underestimating.

You cost somebody a lot of time/money; you almost cost Steve Jackson Games their existence; you got several folks arrested for receiving stolen goods (in essence); you endangered a lot of bulletin boards and maybe even BBS nets in general. Please find some other way to prove how great you are, OK?"

In other words, ignorance is bliss? Don't show the world how fragile and vulnerable all of this information is and somehow everything will work out in the end? We have a lot of trouble with that outlook. Incompetence and poor design are things that should be sought and uncovered, not protected.

***

"I've just read the rather long article describing the investigations of BBS systems in the US. While the actions taken by the investigators sometimes seemed extreme, I would ask you to consider the following simple analogy:

'If you see the front door of someone's house standing open, do you feel it's appropriate to go inside?'

See, it's still a crime to be somewhere you're not supposed to be, whether damage is done or not. Wouldn't you be upset if you found a stranger lurking about your house? It's a violation of privacy, pure and simple.

As to the argument that people are doing corporations a 'service' by finding security loopholes, rubbish. Again, would you appreciate a person who attempts to break into your house, checking to see if you've locked your windows, etc.? I think not.

The whole issue is very easily summarized: it's not your property, so don't go near it."

***

"I have not sent along my phone number since there are a few people out there who would try to retaliate against my computer for what I am going to say.

I have not read such unmitigated BS since the last promises of Daniel Ortega.

You object to the 'coming through my front door and rummaging through my drawers' analogy by mentioning leaving the front door open. In the first place, by what right do you enter my house uninvited for any reason? That can be burglary, even if all you take is a used sanitary napkin. (By the way, in Texas, burglary of a habitation (house) is a first degree felony 5 to 99 or life). Burglary is defined as the entry of a building with the intent to commit a felony or *theft*. Entry of or remaining on property or in a building of another without the effective consent of the owner, is criminal trespass and can get you up to a year in the county jail. When you go into someone's property, even electronically, you are asking for and *deserving* of punishment if you get caught.

Is the nosy 14-year-old going to be any less dead if the householder sees him in the house at 3:00 am and puts both barrels of a 12 gauge shotgun through him? (Not knowing that the late 14-year-old was only there 'to learn'.) As to storming into a suspect's house with guns etc., what the hell are they supposed to do? Take the chance that the individual is armed with an assault rifle?

As to the *Phrack* case, I have read the indictments, and if the DOJ can prove its case, these individuals (one called by his own counsel 'a 20-year-old nebbish') deserve what they get. Neidorf had to know the material he published was private property, and the co-defendant who cracked the Bell South files, had to know he had no right to do so. The fact that much of the information was publicly available from other sources is both immaterial and irrelevant. Is it any less theft if you steal my encyclopedia rather than my silverware?

(continued on page 39)

(continued from page 19)

using NETLINK, type Q or QUIT to return to PRIMOS. If you would like to see the other commands (yeah, there are more) that I am not covering in this article, then type HELP. You've got the basics down now, so go fiddle around with NETLINK and see what other strange things you can do.

Texts for Clearing Cause Codes detected by NETLINK

0 0 DTE Originated
1 0 Busy
3 0 Invalid Facility Request
5 0 Network Congestion
9 0 Out Of Order
11 0 Access Barred
13 0 Not Obtainable

"On these archaic revisions of PRIMOS you can enter CTRL-C as the password of a valid account and automatically bypass the front door password security."

17 0 Remote Procedure Error
19 0 Local Procedure Error
21 0 Out Of Order
25 0 Refusing Collect Call
33 0 Incompatible Destination
41 0 Fast Select Acceptance Not Subscribed
57 0 Ship Absent
128 0 DTE Originated (Non-standard Diagnostic)
129 0 Busy (Private)
131 0 Invalid Facility Request (Private)
133 0 Network Congestion (Private/Routethrough)
137 0 Out Of Order (Private/Routethrough)
139 0 Access Barred (Private)
141 0 Not Obtainable (Private)
145 0 Remote Procedure Error (Private)
147 0 Local Procedure Error (Private/Routethrough)
149 0 RPOA Out Of Order (Private)
153 0 Refusing Collect Call (Private/Primenet)
161 0 Incompatible Destination (Private)
169 0 Fast Select Acceptance Not Subscribed (Private)
185 0 Ship Absent (Private)
193 0 Gateway-detected Procedure Error
195 0 Gateway Congestion

Texts for Diagnostic Codes detected by NETLINK

0 0 No additional information
1 0 Invalid P(S)
2 0 Invalid P(R)
16 0 Packet type invalid
17 0 Packet type invalid - for state r1
20 0 Packet type invalid - for state p1
21 0 Packet type invalid - for state p2
22 0 Packet type invalid - for state p3
23 0 Packet type invalid - for state p4
24 0 Packet type invalid - for state p5
26 0 Packet type invalid - for state p7
27 0 Packet type invalid - for state d1
29 0 Packet type invalid - for state d3
32 0 Packet not allowed
33 0 Unidentifiable packet
36 0 Packet on unassigned logical

channel
38 0 Packet too short
39 0 Packet too long
40 0 Invalid GFI
41 0 Restart with nonzero in bits 1-4, 9-16
42 0 Packet type not compatible with facility
43 0 Unauthorized interrupt confirmation
44 0 Unauthorized interrupt
48 0 Timer expired
49 0 Timer expired - for incoming call
50 0 Timer expired - for clear indication
51 0 Timer expired - for reset indication
52 0 Timer expired - for restart indication
64 0 Call setup or clearing problem
65 0 Facility code not allowed
66 0 Facility parameter not allowed
67 0 Invalid called address
68 0 Invalid calling address
69 0 Invalid facility length
70 0 Incoming call barred
71 0 No logical channel available
72 0 Call collision
73 0 Duplicate facility requested
74 0 Nonzero address length
75 0 Nonzero facility length
76 0 Facility not provided when expected
77 0 Invalid CCITT-Specified DTE facility
112 0 International problem
144 0 Timer expired
145 0 Timer expired - For interrupt confirmation
160 0 DTE-Specific Signal
163 0 DTE Resource constraint
239 0 User segment deleted
240 0 Time out on clear request
241 0 Time out on reset request
242 0 Time out on call request
243 0 Routethrough down
244 0 Routethrough - not enough memory
245 0 Routethrough - circuit timeout
246 0 Routethrough - call request looping
247 0 Routethrough protocol error
248 0 Network server logged out
249 0 Local procedure error Primenet. internal
250 0 Host down
251 0 Illegal address
252 0 No remote users
253 0 System busy
254 0 System not up
255 0 Port not assigned

Other Useful PRIMENET Utilities

There are two other useful PRIMENET utilities, and these are MONITOR_NET and CONFIG_PRIMENET. In this section I will briefly detail these two utilities.

CONFIG_NET is useful for obtaining such information as intra-system links (disk partitions that are shared by systems on a PRIMENET ring), remote login passwords, and system NUA's. Just type:

*OK, **config_primenet configfilename***

The "configfilename" is the name of the PRIMENET configuration file (located in the *>PRIMENET* directory from MFD 0. You can *really* screw up a PRIMENET ring with this utility, so be careful. You don't want to *ever* save a modified configuration. Always answer such a question with NO. The only command you will really ever need to use is the LIST command. When you type LIST it will ask you what you want to list. Just type ALL and it will list all available information regarding the PRIMENET configuration. CONFIG_PRIMENET has a HELP facility available, so use it.

MONITOR_NET is a useful utility for network freaks. It allows the complete monitoring of the local PRIMENET ring network, all virtual circuits, synchronous lines and LAN300 status. You cannot monitor type-ahead buffers or anything, but you can learn quite a bit about the systems on the ring. It will allow you to discover which nodes on the PRIMENET ring/LAN300 do a high amount of data transfer, user ID's on individual systems (albeit no passwords), etc.

Unfortunately, MONITOR_NET is an emulation-dependent utility. Most Prime utilities support the PT series of emulation (Prime Terminal), but most of you will not have access to a terminal program that supports it. Prime was smart in one important regard, and that is that not all of their customers will be using the PT emulation, so they made MONITOR_NET able to understand other popular emulations, such as VT100. Defaultly, MONITOR_NET assumes you are using PT100 or a similar mode of PT emulation. To tell it that you are using VT100, you must use the -TTP argument (terminal type) on the PRIMOS command line. To invoke MONITOR_NET with VT100 emulation, you would type this:

*OK, **monitor_net -ttp vt100***

Upon invoking MONITOR_NET, the screen will clear and you will be presented with a menu of options. MONITOR_NET is really easy to use (just make sure you enter all the commands in UPPER case), so just play around with it.

Miscellaneous Bits

The Physical System Console

The physical system console of a Prime computer has added power over any other local or remote terminal. It is only from this one specific console that several potent operator commands can be issued and invoked successfully.

A few of these console-specific commands will be boring to any hacker not into system programming on a Prime. Some commands, however, will be rather useful. About the most useful console command is the "RESUS -ENABLE" command. As you might recall from Part Two, RESUS is the REmote System USer facility. That is to say, when RESUS is enabled and you are logged into an administrator account, you will actually be a virtual system console. This will allow all console commands to be able to be used from any local or remote terminal. The -ENABLE argument simply tells PRIMOS that you want to turn RESUS on.

Another useful console command is the user logoff command. With this you will be able to logoff users other than yourself. This is not advised.

Also useful are the log management commands. These will allow you to make your presence on the system virtually unknown. Simply edit all logs, both PRIMOS and NETWORK related, and kill all references to yourself. There is much that you can do. For a full list of operator commands you will have to invoke the online HELP facility by typing, you guessed it, HELP. Without an argument, it should list all the PRIMOS commands. Just pick out those that say "Operator Command" beside them.

I'm not really going to continue with this topic as you will have a hard time getting console capability unless you are on-site or the fools have RESUS enabled and you are using a SYS1 priv'ed account. You don't need the logging commands to edit the logs (just the SYS1 privs). Lastly, there are ways of getting console that I will not discuss. I just want you to know that there are additional methods available and that you

should work at finding them. It's the best way to really learn (besides, it's too sensitive to release to the general hacker community).

"One need not be malicious to learn."

Hacking Older (Outdated) Revisions of PRIMOS

I hadn't planned on covering any pre-19.x.x revisions of PRIMOS, but I thought some of you avid network hackers might be interested to know the very basics about these insecure revisions.

Revisions 18.x.x, 17.x.x, and earlier will actually tell you whether or not a given user ID is valid before asking you for a password. This makes it a rather trivial task of determining whether or not a given account exists. In my experiences, early revisions of PRIMOS will be found only on obscure nets, like those in Brazil and Japan. On these archaic revisions of PRIMOS you can enter CTRL-C as the password of a valid account and automatically bypass the front door password security. Very nice. You can barely find these ancient revisions anymore.

These older revisions are not at all like the current revisions of PRIMOS. I suggest reading the "Hacking PRIMOS" article by Nanuk of the North if you plan on penetrating these revisions, as his file was written in the days when 18.x.x was common.

Not really much more that I can say, as you'll probably never come across these revisions and even if you do, the command structure they use is enough to cause severe gastro-intestinal disorders.

Simplified Means of Attaching to Sub-UFD's

Sub-directories are great, but when you start going deeper than two levels on a Prime it starts getting to be a pain. Full pathnames get to be depressing when you are six or seven levels deep. Enter the UP and DOWN external commands. Recall that I mentioned these commands earlier in the series. These externals are found on most Primes, but there are a few that do not have them available.

Note: I did not write these utilities. Many versions exist on different systems. I have yet to see copyright notices, so I will assume that they are either examples from the CPL Reference Manual or public domain.

DOWN.CPL SOURCE CODE

```
/* DOWN.CPL, DOWN_ATTACH, WHO_KNOWS, 02/24/89
/* An external command to simplify down-ATTACHing.
/*
/* START-CODE:
/*
  &args path
  &do &while [null %path%]
    &s path := [response 'UFD to Down-ATTACH to' ']
  &end
  a *>%path%
  type Now attached to %path%
  &return
/*
/* END-CODE
```

UP.CPL SOURCE CODE

```
/*    UP.CPL,    UP_ATTACH, WHO_KNOWS, 02/24/89
/* An external command to simplify up-ATTACHing.
/*
/* START-CODE:
/*
```

(continued on page 46)

NEWS UPDATE

It appears that the times may indeed be changing. For years, we've encouraged our readers to battle the unfair fees on touch tones that the phone companies charge. Now comes word out of California that Pacific Bell's latest rate proposal calls for the elimination of touch tone service charges. We understand they're not the first and we doubt they'll be the last....In New York, plans are underway to add another area code in the next couple of years. The interesting thing here is that this code (917) would be used for one part of the city (The Bronx) plus cellular phones, beepers, and voice mail systems in Manhattan. How this is all going to be coordinated should be loads of fun....What's the largest local phone company in the United States? Nynex? Ameritech? Bell South? No, GTE. That's right, a non-Bell company will be the largest in the country, once it acquires Contel, another independent phone company. GTE currently operates local service in 46 different states, Contel in 30....Nynex is planning on buying AXE digital switches from Ericsson and locating them in the 914 area code. We're not aware of any AXE switches currently operating in the U.S. If you happen to know of one, let us know....AT&T has been operating a service called Voicemark, which allows you to send messages to people by phone at a designated time by calling 800-562-6275 and giving them your calling card number or Visa/Mastercard. The charge is $1.75 for a one minute message to any phone in the country....Metromedia/ITT probably has the best phrasing in their calling card instructions: "simply *swipe* your card through the slot"....US Sprint has a new solution for prison inmates. Instead of forcing inmates to make collect calls, Sprint provides a service called "Safe Block". Inmates must establish a long distance fund that they draw upon whenever making a call. Calls can only be made to predetermined numbers and the inmate is identified with a 9 digit authorization code....Get ready for some neat acronyms: British Telecom (BT) has won a major contract from the government for private branch exchanges (PBX's) for use in emergencies. In order to get the contract, their PBX had to be able to withstand the electro magnetic pulse (EMP) that comes with a nuclear explosion (SOL). BT states that EMP would have a catastrophic effect on computerized equipment. So far they don't seem to have developed a plan to protect any people....BT also has acronyms for new services they're providing. Calling Line Identity (similar to Caller ID here) is known as CLI. Their version of Call Trace is called Malicious Call Identification, or MCI!....Finally from England: BT payphones no longer take 2p or 5p coins. That was phased out in June. But the phones still take 10p, 20p, 50p, and one pound coins. But it won't be as much fun. That's because payphones there work very differently from payphones here. All calls carry a minimum charge of 10p. But unused coins are returned. So you can put two 10p coins in and if the display only goes down 3p, one of your 10p coins will be returned. But this can get quite interesting. Let's say you've put a 20p coin in the phone and the display is down to 5p. By quickly inserting a 10p and a 5p coin, you've overpaid by 20p, so the 20p coin comes out. In actuality you would have saved 5p that otherwise would have been swallowed. It's pretty obvious how BT will benefit from this since the above example will no longer be possible. This shadiness is similar to the way Bell-operated payphones ask for a nickel for the next several minutes (for local calls, not long distance) and credit whatever you put in as a nickel, even if it's a quarter. We know they have the technology to tell the difference. But there's no incentive for them to use it in this case. So maybe the times really aren't changing after all....

NEGATIVE FEEDBACK

(continued from page 33)

But, breaking into a computer is not walking through an unlocked door. Access by unauthorized people is only through an act which is illegal in itself. Whether the motive for the act is good, evil, or indifferent is of no consequence. *You have no right to enter my computer without my authority than you do to enter my house!* You seem to have the idea that if the entry is for experiment or fun and not for profit, then it is OK. Bullshit, and you know it.

You say you've been hacked yourself - and *you* blame the people who sold you the product or service, not the hacker. You would blame the Jews in the 40's, not the SS?

Also, if someone breaks into my office and only reads the files of my clients - doesn't take anything - has he harmed them by seeing information that is none of his damned business?

What we've got is one more expression of the 'spoiled brat syndrome'. 'I can do it, so I may do it and don't you dare punish me if I get caught.' Children, I have news for you! I catch you in my house at 3:00 am, I'll fill your ass so full of buckshot you'll walk like a duck for the rest of your life. I catch you in my computer, I'll have the Secret Service on you like ugly on an ape.

A corporation has the same right to privacy as an individual. Due to business necessity, they may have to leave their computers on 24 hours a day. Where is it written that any asshole who can figure his way into the company's computer can do so with impunity? More fittingly, if he is caught, he should be publicly flogged, as I do not like the idea of supplying him with three hots and a cot for five to life.

I might add that in Texas, *any* unauthorized entry to a computer is a crime and can be anything from a Class B misdemeanor to a third degree felony depending on the circumstances - that works out at anything from one day to ten years in *jail*. Some fun and games."

We'd sure like to see what kind of responses these letters elicit from our readers. In fact, we'll give away a free 2600 lifetime subscription to the person who writes the best reply to the points raised here. (If you're a current lifer and you win, you can have a lifetime subscription sent to a friend.) Submissions should be between 3-5 pages doublespaced without too many obscenities. Send them to 2600 Contest, PO Box 99, Middle Island, NY 11953. You've got until the end of the year.

Too risky to mail?
Too paranoid to speak its name?
Then FAX it!
516-751-2608

phrack on trial

(continued from page 7)

pulling out once they realized a mistake had been made. Of course we would have preferred it if they had recognized their mistake earlier in the process, but at least they didn't ignore it and try for one guilty verdict on any of the other counts.

If we were bitter conspiracy theorists, we'd probably suggest that the government knew this case was a waste from the very beginning, but chose to pursue it as a means of harassing (financially and emotionally) Neidorf (and by association the rest of the C.U.). However there is little to indicate that this is true, and there is no reason to doubt the sincerity, albeit misinformed, of Cook et al. (As the old saying goes, do not attribute to malice that which can be adequately explained by stupidity.)

Finally, the long term effects of this case, if any, remain to be seen. The Secret Service is still in possession of much computer equipment and seized belongings. While we don't expect the decision in Neidorf's trial to have any ramifications for the other investigations (Neidorf, after all, wasn't a hacker himself), we do wonder if perhaps the cries of "C.U. conspiracy" and "communist plot" will subside. Perhaps this will allow everyone a moment to reassess their assessment of the danger the C.U. represents.

First Amendment issues connected with this case, and their implications for *2600*, *TAP*, *PHUN*, and even *C-u-D*, have not been decided. Judge Bua struck down a pre-trial motion (filed by the E.F.F.) on the 1st Amendment and unfortunately that "ruling" is the only Constitutional debate that ever came to a head. Neidorf won't be the test case for this issue, but eventually someone will. Let's hope that in the interim some other electronic publishing case will set a precedent on this...hopefully one that covers a topic that is not the lightning rod the C.U. seems to be.

NEIDORF DEFENSE FUND
Katten, Muchin, & Zavis
525 West Monroe St, #1600
Chicago, IL 60606-3693
Attn: Sheldon Zenner

COUNT TWO

"...defendant herein, for the purposes of executing the aforesaid scheme did knowingly transmit and cause to be transmitted by means of a wire and radio communication in interstate commerce from Columbia, Missouri to Lockport, Illinois certain signs, signals and sounds, namely: a data transfer of Phrack World News announcing the beginning of the "Phoenix Project" in violation of Title 18, United States Code, Section 1343.

==Phrack Inc.==

Volume Two, Issue 19, Phile #7 of 8

From The Creators Of Phrack Incorporated...

The Phoenix Project

Just what is "The Phoenix Project?"

Definition: Phoenix (fe/niks), n. A unique mythical bird of great beauty fabled to live 500 or 600 years, to burn itself to death, and to rise from its ashes in the freshness of youth, and live through another life cycle.

Project (projekt), n. Something that is contemplated, devised, or planned. A large or major undertaking. A long term assignment.

Why is "The Phoenix Project?"

On June 1, 1987 Metal Shop Private went down seemingly forever with no possible return in sight, but the ideals and the community that formed the famous center of learning lived on. On June 19-21, 1987 the phreak/hack world experienced SummerCon'87, an event that brought much of the community together whether physically appearing at the convention or in spirit. On July 22, 1987 the phreak/hack community was devastated by a nationwide attack from all forms of security and law enforcement agencies...thus setting in motion the end of the community as we knew it. Despite the events of July 22, 1987, PartyCon'87 was held on schedule on July 26-28, 1987 as the apparent final gathering of the continent's last remaining free hackers, unknown to them the world they sought to protect was already obliterated. As of August 1, 1987 all of the original members and staff of the Metal Shop Triad and Phrack Inc. had decided to bail out in the hopes that they could return one day, when all would be as before...

THAT DAY HAS COME...

A new millennium is beginning and it all starts on July 22, 1988. How fitting that the One year anniversary of the destruction of the phreak/hack community should coincidentally serve as the day of its rebirth.

Announcing SummerCon '88 in (where else would you expect) St. Louis, Missouri!

Knowledge is the key to the future and it is FREE. The telecommunications and security industries can no longer withhold the right to learn, the right to explore, or the right to have knowledge. The new age is here and with the use of every "LEGAL" means available, the youth of today will be able to teach the youth of tomorrow.

SummerCon'88 is a celebration of a new beginning. Preparations are currently underway to make this year's convention twice as fun as last year's and the greater the turnout the greater the convention shall be. No one is directly excluded from the festivities and the practice of passing illegal information is not a part of this convention (contrary to the opinions of the San Francisco Examiner, and they weren't even at the last one). Anyone interested in appearing at this year's convention should leave mail to Crimson Death immediately so we can better plan the convention for the correct amount of participants.

The hotel rooms purchased for SummerCon'88 are for the specified use of invited guests and no one else. Any security consultants or members of law enforcement agencies that wish to attend should contact the organizing committee as soon as possible to obtain an invitation to the actual convention itself.

Sorry for the short notice this year...

:Knight Lightning

"The Future Is Forever"

The above would have been good for a $1000 fine and up to five years in prison, if Neidorf had been convicted. Welcome to the nineties.

2600 Marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011,212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

NEW FROM CONSUMERTRONICS: "Voice Mail Hacking" ($29), "Credit Card Scams II" ($29), Credit Card Number Generation Software (inquire). More! Many of our favorites updated. New Technology Catalog $2 (100 products). Need information contributions on all forms of technological hacking: 2011 Crescent, Alamogordo, NM 88310. (505) 434-0234.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

RARE TEL BACK ISSUE SET. (Like TAP but strictly telephones.) Complete 7 issue 114 page set $15 ppd. TAP back issue set-320 pages-full size copies NOT photo-reduced $40 ppd. Pete Haas, P.O. Box 702, Kent, Ohio 44240.

VIRUSES, TROJANS, LOGIC BOMBS, WORMS, and any other nasties are wanted for educational purposes. Will take an infected disk and/or the source code. If I have to, I will pay for them. Please post to: P. Griffith, 25 Amaranth Cn, Toronto, ONT M6A 2P1, Canada.

WANTED: Audio recordings of telephone related material. Can range from recordings of the past and present to funny phone calls to phone phreaking. Inquire at 2600, PO Box 99, Middle Island, NY 11953. (516) 751-2600.

VMS HACKERS: For sale: a complete set of DEC VAX/VMS manuals in good condition. Most are for VMS revision 4.2; some for 4.4. Excellent for "exploring"; includes System Manager's Reference, Guide To VAX/VMS System Security, and more. Mail requests to Roger Wallington, P.O. Box 446, Leonia, NJ 07605-0446.

WANTED: Red box plans, kits, etc. Also back issues of Phrack, Syndicate Reports, and any other hack/ phreak publications, electronic or print wanted. Send information and prices to Greg B., 2211 O'Hara Dr., Charlotte, NC 28273.

TAP MAGAZINE now has a BBS open for public abuse at 502-499-8933. We also have free issues. You send us a 25 cent stamp and we send you our current issue. Fancy huh? Mail to TAP, P.O. Box 20264, Louisville KY 40250-0264.

SUBSCRIBE TO CYBERTEK, a magazine centered upon technology with topics on computer security. Send $10 for a one year subscription to Cybertek Magazine, PO Box 64, Brewster, NY 10509.

NEEDED: Info on speech encryption (Digicom, Crypto). Send to Hack Tic, P.O. Box 22953, 1100 DL, Amsterdam, The Netherlands.

CYBERPUNKS, HACKERS, PHREAKS, Libertarians, Discordians, Soldiers of Fortune, and Generally Naughty People: Protect your data! Send me a buck and I'll send you an IBM PC floppy with some nifty shareware encryption routines and a copy of my paper "Crossbows to Cryptography: Techno-Thwarting the State." Chuck, The LiberTech Project, 8726 S. Sepulveda Blvd., Suite B-253, Los Angeles, CA 90045.

WANTED: Red box kits, plans, and assembled units. Also, other unique products. For educational purposes only. Please send information and prices to: TJ, 21 Rosemont Avenue, Johnston, RI 02919.

FOR SALE: Manual for stepping switches (c) 1964. This is a true collector's item, with detailed explanations, diagrams, theory, and practical hints. $15 or trade for Applecat Tone Recognition program. FOR SALE: Genuine Bell phone handset. Orange w/tone, pulse, mute, listen-talk, status lights. Fully functional. Box clip and belt clip included. $90 OBO. Please post to S. Foxx, POB 31451, River Station, Rochester, NY 14627.

Deadline for Fall Marketplace: 10/1/90.

HOW TO MAKE COCOTS

(continued from page 23)

Some DTMF based COCOTs are simply activated with a single silver box tone (see Winter 1989-90 issue of *2600*). I've run into a couple of these.

To play around with the remote functions of a COCOT, if they exist in the particular model, it is necessary to obtain the phone number of the unit. See the next section on that. Once you have the number, simply call it, and experiment from then on. If you have trouble hacking the formats for the remote mode, it may be necessary to call the makers of the COCOT and social engineer them for the information.

Getting the COCOT's number

This is incredibly trivial, but is included here because it is such an important function in the exploration/abuse of any COCOT, and because advanced COCOT exploration/abuse techniques will require you to have this information. It is also included here for the novice reader.

There are several ways to obtain the phone number, the simplest being dialing your local ANAC number, plus dummy digits if necessary. A lot of COCOTs will restrict this, so you should get an unrestricted dialtone and then dial ANAC. Some COCOTs will not restrict you, but will ask for money in order to do this. Here in NYC, dropping $.25 and dialing 958-1111 will get you the ANAC readout on this type of COCOT. A small price to pay for such valuable information. Another way to obtain the number is to get it from the operator. Any operator that has it will have no problem releasing it to you; just say you're calling from a payphone, and you need someone to call you back, but there is no phone number written on the payphone. Yet another choice is to call one of the various ANI Demo 800 numbers, which will read back your number. This choice is particularly useful for people who don't have or don't know the ANAC for their area. If in desperation, social engineer the information out of the COCOT owner, call him up as the phone company, and take it from there.

Hijacking the Bastard

Besides using the COCOT to make calls, the typical phone phreak will usually want a COCOT for himself. Granted, this is stealing, but so is not paying for calls. And while we're at it, stealing for experimentation and the pursuit of knowledge is not the same as stealing for money. Oh well, I won't get into morals here, it's up to you to decide. Personally, I'm devoid of all ethics and morals anyway, so I'd steal one if the opportunity was there. What the heck, it can't be any worse then exercising your freedom of speech and being dragged off to jail by the fascist stooges of the imperialist American police state. Ahem, sorry about that, I got a little carried away, but I just had to comment on events of the past several months.

"You can be sure that most calls placed on COCOTs have an extremely large amount of static and bizarre echoing effects."

Anyway, the reasons for abducting a COCOT range from simple experimentation ("I'd like to see what the hell is in there.") to purely materialistic reasons ("Hmmm. I bet that coin box holds at least $10."). Whatever the reason, a COCOT is a good thing to have. Their retail value ranges from $900 to $2500, but since you can't really re-sell it, I wouldn't suggest taking one for purely materialistic reasons.

WORK FOR YOU

Abducting a COCOT is usually much easier than trying to do the same to a real payphone. Physical security can range widely and depends largely on the owner. I've seen security ranging from a couple of nails fastening the COCOT to a sheet of plywood, to double-cemented bolted down steel encasements. However, a crowbar will do the trick for about 50% of the COCOTs in my area. Expect the same wherever you are.

Once obtained, your options vary. You could take it apart, you could hang it on your bedroom wall, you could hold it for ransom, it's up to you. Most people simply connect it up to their line, or hang it up as a trophy above the mantle. As you can tell from the introduction, dissecting the COCOT will yield you a plethora of interesting devices to keep you busy for a long time to come. If you do connect a COCOT to your line, be sure to tape up the coin slot, as placing money in the COCOT, without an ability to remove the coin box will eventually choke the unit. Don't use it as a primary phone, since it demands money; it's neat to have it as an extension.

Destruction

If you can't steal it, and you can't (ab)use it, destroy it.... That's my motto with regard to COCOTs. These evil beasts have been ripping off the public for a long time, and they deserve to pay the price. Destruction can range from breaking off plastic forks in the coins slot, to removing the handset (for display as a trophy of course), to completely demolishing the unit with explosives, to squeezing off a few shotgun blasts at the COCOT. Since repair and/or refund is hard to come by and expensive when it comes to COCOTs (but is free for real payphones), the COCOT owner will think twice before purchasing another COCOT.

The Phone Line

As mentioned earlier, the phone line used by the COCOT is just a regular line. It is usually exposed near the COCOT itself. For those of you with a lineman's handset, need I say more? For those without, let me just quickly say, get your hands on one.

Advanced Techniques

The next three sections are for the more experienced phone phreak, but most of this can be done by just about anyone. There are many more advanced techniques, the boundaries are limitless.

Code Theft

As mentioned earlier, most COCOTs use various small and sleazy long distance companies and operator assistance services (ITI, Telesphere, Redneck Telecom, etc.) for long distance, collect, third-party, and calling card calls. Many times these are accessed by the COCOT through a 1-800, 950, or 10XXX number. The COCOT dials the access number, its identification number or code, plus other information in order to use the service. The service then bills the COCOT owner (or the middleman re-seller of COCOT services) for the services provided but not yet paid for. In the case of calling card calls or collect calls, the service bills the proper party through equal access billing and credits the COCOT owner's account a cut of the action.

Needless to say, all the DTMF tones required to access the service can be taped and decoded (see the DTMF decoder article in the Spring 1990 issue of *2600*), and used for our own purposes. Sometimes, you can tape the tones right from the handset earpiece, other times, the handset is muted, and it is required for you to either access the wiring itself, or trick the phone into thinking that your called party hung up, and you're making another call, while having the party on the other end give a bogus dialtone to the COCOT and tape the forthcoming tones. Surprisingly the codes obtained from this type of activity last a very long time (usually 3-4 months). This is because, once the charge gets all the way down the chain, through the various middlemen and re-sellers, to the COCOT owner, and by the time the COCOT owner realizes that the coins collected don't match the calls placed, and by the time he has to convince all the middlemen above him of possible fraud...well, you get the picture, suffice to say, these codes last. Used in moderation, they can last for a long time, because the COCOT owner is raking in so much profit, he'll easily ignore the extra

calls.

Calling Card Verification

With regard to messing around with Calling Card verification, I could write a whole separate article on this, but space does not allow it at this time. So, I'll just give you the basics.

Much of the Calling Card verification that's being done by sleazy long distance and AOS services is very shabby. Since access to AT&T's calling card database for verification is expensive for these companies, they try to do without. Much of the time, they don't verify the card at all, they make sure it looks valid (a valid area code and exchange), and simply throw out the PIN, thus assuming the card is valid. A valid assumption, given that more than 95% of the calling cards being punched into COCOTs are valid, it's a worthwhile risk to take. However, the shit hits the fan when someone receives his bill, and sees that he has a bunch of calling card calls on his bill, and he doesn't even have a calling card! Fraud is reported, the bureaucracy churns, until finally, the sleazy long distance company ends up paying for the call. Given enough of these calls, these companies get hell from AT&T and the RBOCs for not properly verifying calling card numbers. The FCC gets into the act, and the company pays fines up the wazoo. A pretty good thing, if you ask me, and you get a free call out of it as well. Not a bad transaction, not bad at all....

Other long distance companies and AOS services steal verification services from AT&T by dialing a 0+ call on another line to a busy number, using the calling card number you punched in. If it receives a busy signal, the card is good, otherwise it is not. In either case, the long distance company eludes the charge for accessing the database. When it comes to slinging sleaze, these companies deserve an award. And that's why I urge all out there to abuse the crap out of them.

Call Forwarding

This is another of the many interesting things that can be done with your neighborhood COCOT. Simply put, you get the phone number to the COCOT, call up your local phone company, order call forwarding for that line, then go to the COCOT and forward it to your number. A lineman's handset may be required here, if you can't get your hands on an unrestricted dialtone. Pulling a CN/A or doing some research may be required if your local phone company asks a lot of information before processing such requests as call forwarding. In most cases they don't, and in some areas there are automated facilities for processing such requests.

Presto! You now have an alternate number you can use for whatever purpose you have in mind. It could be used from anything to getting verified on a BBS to selling drugs. Again, your ethics are your own; this is simply a tool for those who need it. Anyway, it's practically untraceable to you as far as conventional means are concerned (CN/A, criss-cross directory, etc.), and you should use it to your advantage. This is especially a good tool for people afraid to give out their home numbers.

At any time, you can go to the COCOT and de-activate the call forwarding to your number. Since no one ever calls the COCOT, except for using the remote mode, and this is rare and mostly used when the phone is broken, you should have few if any calls intended for the COCOT. If you do get a call from a COCOT service bureau, simple say "wrong number", go to the COCOT, and de-activate call forwarding for a few days, just to be safe. In any case, your real number cannot be obtained through any conventional means by those calling the COCOT, or even by those standing at the COCOT itself. However, if they really wanted to nail you, they could examine the memory at the COCOT's switch and pull your number out of its call forwarding memory. However, I have never heard of this being done, and it's very unlikely that they would do this. But I wouldn't recommend using the alternate

number for anything more than an alternate number for yourself. If you sell drugs or card stuff or something like that, don't use such an alternate number for more than a few days.

The Future of the COCOT

We're definitely going to see many more COCOTs in the future. They will begin to saturate suburban and rural areas, where they can rarely be found at this time. More COCOTs mean more headaches for the public, but it also means more of us will get a chance to experiment with them.

"Much of the Calling Card verification that's being done by sleazy long distance and AOS services is very shabby."

Security, both physical, and anti-phreak will get better, especially after COCOT manufacturers read this article. But it will be a long time before we will see completely secure COCOTs. Which is not so bad really, because then they will actually be worth stealing.

In the meantime, we can decrease their proliferation by destroying any COCOTs that rip people off. Having COCOTs around is a bitter-sweet proposition. In a way, they are an interesting use of technology and another frontier of exploration for the phone phreak. On the other hand, they are cybernetic money-leeching abuses of technology, which steal from and abuse the public they are meant to serve. Like 'em or not, they're here to stay.

Getting More Info

For those of you who wish to find out more about COCOTs, I would recommend hands-on exploration. I would also recommend getting some of the COCOT industry publications, and various telephone industry publications. You could also request more information from COCOT manufacturers themselves, Intellicall being one of the largest. Also, check out government and FCC regulations with regard to equal access and COCOTs.

Fighting the Bastards

Much of the stuff being perpetrated by COCOTs today is against the law, and the sleazy companies that handle calls for COCOTs are violating many laws. Unfortunately, few of these laws are being enforced. When you see such a violation of consumer rights, please report it to all relevant agencies. You'll know you're being taken advantage of when someone calls you collect from a COCOT and you get charged up the wazoo for the 10 minute local call. And they call us criminals. Give me a break....

The only way to control these cybernetic leeches is to do something about them. Also, if you have a grudge against a COCOT or a sleazy company, by all means take the law into your own hands. But also, write to your legislators, complaining of the abuses being perpetrated by COCOTs and the sleazy telephone companies. Also, it is important to educate the public about COCOTs and how to recognize and avoid them, whenever possible try to inform your non-phreak friends about the dangers of using COCOTs. I am also in favor of strict regulation when it comes to the subject of COCOTs. If they must charge insane rates, these rates should be stated clearly, and they must provide quality service, clear connections, and free operator assistance. Anything less than this is unacceptable.

In closing, I would just like to say that this article is as complete as my knowledge enables it to be. It by no means explains all there is to know about COCOTs, nor do I claim to know all there is to know. If you have any other information on COCOTs or any particularly tasty COCOT stories, please write to 2600, and tell us more.

PRIME CONCLUSIONS

(continued from page 37)

```
&args num:dec=1
&s path := [dir [pathname *]]
&do I := 1 &to %num%
  &s path := [dir [pathname %path%]]
&end
a %path%
type Now attached to %path%
&return
/*
/* END-CODE
```

Conclusion

All in all I find the PRIMOS operating system excellent, both in power and in user friendliness. One can do almost anything from PRIMOS and its associated utilities and language systems. It's every bit as capable as VAX/VMS or UNIX.

Primes have, on the down side, become a lot more difficult to hack. Prime Computer, Inc. has become aware of the increasing popularity of PRIMOS with hackers and has taken the appropriate steps in alerting its customers. This probably has already affected you. Defaults are gone. System passwords are in effect. Increased system security. This makes hacking Prime computers these days a damn sight more difficult than it once was. To this you may thank all those people that abused NETLINK on PRIMENET systems and so forth.

Enjoy a Prime when you get in one. Experiment with the operating system. Most of all, however, *learn!* One need not be malicious to learn. When experimenting, experiment on *your own* filesystems, not those of the owners. As I have said, it is more difficult to obtain PRIMOS and PRIMENET accounts these days. Cherish and benefit from them, but do not act like an idiot and end up making it harder for everyone else.

References

FDR3108-190L (PRIMOS Commands Reference Guide)
FDR3104-101B (New User's Guide to EDITOR and RUNOFF)
FDR3250 (PRIMOS Commands Programmer's Companion)
FDR3341 (BASIC/VM Programmer's Companion)
Hacking PRIMOS Volumes I and II (by Codes Master)
Hacking PRIMOS I, II, and III (by Evil Jay)
PRIMOS: Networking Communications (by Magic Hassan)
PRIMOS Part I (by Carrier Culprit, LOD/H Tech Journal #2)
PRIMOS (by Nanuk of the North)

Acknowledgements

During the course of the writing of this series many people have lent me their help and support. I now wish to acknowledge those that aided me in this task.

Thrashing Rage - Thanks for the ideas, proofreading, and help in recovering the original documents when the work disk got 164 disk errors. You saved me from two weeks of retyping! Thanks!

The Beekeeper - Thanks for getting the documents to the right people at *2600.*

Mad Hacker - Without all of our hours and hours of discussion this series would not be what it is now. Thanks!

And to all the hackers that have written about the PRIMOS operating system in the past goes a hearty thanks. Couldn't have done it without you guys. Thanks go to: Prime Suspect, Magic Hassan, The Codes Master, Necrovore, Nanuk of the North, and The Force. Thanks guys!

***

May the forces of darkness become confused on the way to your house.

IT'S SIMPLE

In fact, it's never been simpler to renew your subscription to 2600. Just look at your mailing label to find out when your last issue will be. If you have two or fewer issues remaining, it's probably a good idea to renew now and avoid all the heartache that usually goes along with waiting until your subscription has lapsed. (We don't pester you with a lot of reminders like other magazines.) And by renewing for multiple years, you can cheerfully ignore all of the warnings (and occasional price increases) that appear on **Page 47.**

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988,1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED:

ingredients

a bittersweet victory	3
the neidorf/phrack trial	4
an interview with craig neidorf	8
what is the eff?	10
negative feedback	11
primos conclusion	14
fun with cocots	20
letters	24
news update	38
2600 marketplace	41

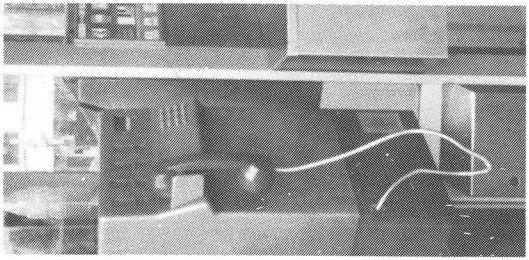
2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

2600

The Hacker Quarterly **$4** *VOLUME SEVEN, NUMBER THREE*
AUTUMN, 1990

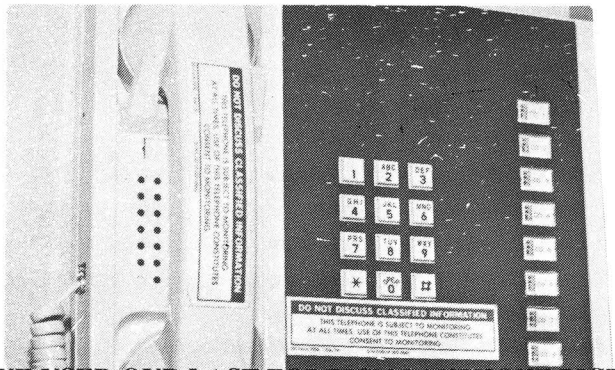
FRENCH COIN PHONES

increasingly hard to find, but here's one in Paris (sideways)



STRANGE DAYS IN HOLLAND

AND MILITARY MADNESS



WE'VE USED OUR LAST FOREIGN PAYPHONE PICTURE!
SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES,
PO BOX 99, MIDDLE ISLAND, NY 11953. HURRY!!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1990, 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada --$18 individual, $45 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESS: 2600@well.sf.ca.us.

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

STATEMENT OF OWNERSHIP MANAGEMENT AND CIRCULATION
U.S. Postal Service
Required by 39 U.S.C. 3685

1A. TITLE OF PUBLICATION	1B. PUBLICATION NO.	2. DATE OF FILING
2600 MAGAZINE		9/26/90
3. FREQUENCY OF ISSUE: QUARTERLY	3A. NO. OF ISSUES PUBLISHED ANNUALLY: 4	3B. ANNUAL SUBSCRIPTION PRICE: $18/$45

4. COMPLETE MAILING ADDRESS OF KNOWN OFFICE OF PUBLICATION (Street, City, County, State and ZIP Code) (Not printers): BOX 752, MIDDLE ISLAND, NY 11953

5. COMPLETE MAILING ADDRESS OF THE HEADQUARTERS OF GENERAL BUSINESS OFFICES OF THE PUBLISHER (Not printer): 7 STRONGS LANE, SETAUKET, NY 11733

6. FULL NAMES AND COMPLETE MAILING ADDRESS OF PUBLISHER, EDITOR, AND MANAGING EDITOR (This item MUST NOT be blank)

PUBLISHER (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953

EDITOR (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953

MANAGING EDITOR (Name and Complete Mailing Address): ERIC CORLEY, 7 STRONGS LANE, SETAUKET NY 11733

7. OWNER (If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address must be stated.) (Items must be completed.)

FULL NAME	COMPLETE MAILING ADDRESS
ERIC CORLEY	7 STRONGS LANE, SETAUKET, NY 11733

8. KNOWN BONDHOLDERS, MORTGAGEES, AND OTHER SECURITY HOLDERS OWNING OR HOLDING 1 PERCENT OR MORE OF TOTAL AMOUNT OF BONDS, MORTGAGES OR OTHER SECURITIES (If there are none, so state): NONE

FULL NAME	COMPLETE MAILING ADDRESS

9. FOR COMPLETION BY NONPROFIT ORGANIZATIONS AUTHORIZED TO MAIL AT SPECIAL RATES (Section 423.12 DMM only)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes: (Check one)
☐ (1) HAS NOT CHANGED DURING PRECEDING 12 MONTHS ☐ (2) HAS CHANGED DURING PRECEDING 12 MONTHS (If changed, publisher must submit explanation of change with this statement)

10. EXTENT AND NATURE OF CIRCULATION	AVERAGE NO. COPIES EACH ISSUE DURING PRECEDING 12 MONTHS	ACTUAL NO. COPIES OF SINGLE ISSUE PUBLISHED NEAREST TO FILING DATE
A. TOTAL NO. COPIES (Net Press Run)	3135	3500
B. PAID CIRCULATION 1. Sales through dealers and carriers, street vendors and counter sales	1000	1150
2. Mail Subscription	1185	1260
C. TOTAL PAID CIRCULATION (Sum of 10B1 and 10B2)	2185	2410
D. FREE DISTRIBUTION BY MAIL, CARRIER OR OTHER MEANS SAMPLES, COMPLIMENTARY, AND OTHER FREE COPIES	22	25
E. TOTAL DISTRIBUTION (Sum of C and D)	2207	2435
F. COPIES NOT DISTRIBUTED 1. Office use, left over, unaccounted, spoiled after printing	928	1065
2. Return from News Agents	0	0
G. TOTAL (Sum of E, F1 and 2 - should equal net press run shown in A)	3135	3500

11. I certify that the statements made by me above are correct and complete

SIGNATURE AND TITLE OF EDITOR, PUBLISHER, BUSINESS MANAGER, OR OWNER: OWNER

PS Form 3526, July 1988

(See instruction on reverse)

CALLER ID:

by Jake "The Snake"

You've probably either heard of it, seen it in the media, or maybe you even own one of those little "buggers". There's been a lot of talk, fighting, and discussions in court over the Caller*ID box. Currently existing only in New Jersey, this device is basically a tracer. And, yes, it is legally available to the public.

In case you aren't aware of such a hacker's dream, let me fill you in on the details. The device itself is a small stand-alone unit, about 6"x4" weighing about 8-10 ounces, with a 32-character (5x8 pixels), 2-line display and a few buttons on the front. In size it resembles a simple desktop calculator from a couple of decades ago. It can run on a 9-volt or A/C adapter and has 2 RJ-11 jacks on the back, both identical, for attachment to wall and phone.

Caller*ID is offered along with many other "sister" services that I will explain later. Because of the AT&T divestiture a few years back, the local companies aren't authorized to sell the device itself but can only offer the service (at a cost of $21 for installation and a whopping $6.50 a month) to its customers. The box can be ordered from a few different distributors for anywhere between $60 and $300.

Let's say you purchased a Caller*ID (known as "ICLID" in the industry, which is an acronym for Incoming Call Line Identification Device) and hooked it up to your phone. This is how it would work: After your phone rings once, you'll see some information flash on the little LCD display. Models vary, but you'll definitely see the caller's phone number and current time and date. Most models store the numbers in memory for recall at any time. So, if you're not around to answer the call, you can be sure that anywhere from 14 to 70 numbers will be saved for your convenience. (It's great to be able to come home and see X number of messages on your answering machine and see X+4 callers on your ICLID. With a little matching up, you can figure out who didn't leave a message.)

Of course, there are drawbacks to our little "mirror box". What are the limitations to its tracing ability? First of all, it won't work without the local company providing the service. Only after the first ring does the information come storming down the line to be decoded by your little friend. (I have two lines in my house, and sometimes there's a bit of crosstalk between them. When the phone rings, if I listen carefully enough I can actually hear the coded ICLID information being sent.) Also, only areas that offer this service (and other "CLASS" Calling Services) to their customers will be traceable areas. But this area is growing.

If someone calls from out of state or from the boonies a message like "Out of Area" will be displayed instead of the number. That's the real bummer. But, all of the latest models of Caller*ID devices are area-code compatible and show your area code where other NPAs will be in the near future. Many states have been slow to pick up the technology mainly because of political and legal reasons. Many privacy issues have been suggested and debated over, but we won't go into those here. As I understand it, New Jersey Bell contends that if a person has your number and calls you, you should have their number as well; when a connection is made, both ends should know who they're talking to. So, hopefully other states will get their asses in gear.

"With the public being offered these services, imagine what business customers, or even Sprint/MCI/AT&T are being offered?"

The option to block particular calls is being juggled around, too. Telephone companies are thinking of offering a service whereby the customer would dial a couple of digits before the 7-digit number and the receiver would get an "Out of Area", or similar, message on their ICLID display. This would definitely suck, unless you are the caller. But, this service is already available now thanks to a small loophole. I'll

THE FACTS

explain later.

New Jersey Bell started CLASS Calling Services around December of 1987. They were test marketed in Hudson County until December, 1988 and then began to spread. Other services include Priority*Call, Call*Block (a personal favorite), Repeat*Call, Select*Forward, Return*Call, Call*Trace, Tone*Block, and others. Many of these are based upon the instant tracing ability of CLASS.

Priority*Call will send you a distinctively different sounding ring when certain people call you. You program a "queue" of phone numbers that when called from, will sound different than the standard phone ringing.

Call*Block is lots of fun. Again, you can program a queue of people into your phone (really, the phone company's computer). When they call your line, they get a recorded message along the lines of, "I'm sorry. The party you have reached is not accepting calls from your telephone number." Nice and rude.

Call*Trace is a service that is available to everyone on a pay-per-trace basis. If you receive a prank, etc., you hang up, pick up, and immediately dial *57. A recording lets you know if the trace was good or bad, and you get charged $1.00 accordingly. Unfortunately you have to call the phone company to get the phone number. This service is for serious complaining and is meant for people who get pranked a lot and want to file charges.

All of the above features can be generally replaced with an ICLID. As a substitute for Call*Block I can simply not answer the phone if I don't want to speak to someone, since my ICLID lets me know who it is. Of course, that pre-recorded message adds a nice touch. Call*Trace is pretty much useless with ICLID unless you want to bring in the gestapo. But, then again, Call*Trace is open for anyone to use and isn't ordered monthly like the other services.

A woman from New Jersey Bell told me, though, some technical legalities regarding Call*Trace and Caller*ID: If someone pranks me, and I return their call (having read their number from my "mirror box") and prank them in return, they can *57 me and sue me for phone harassment. Even though I have their number on my ICLID, if I don't *57 him before I call him back, I get *my* ass kicked in. So, the moral of the story is that ICLID can't be used as evidence of a prank.

Select*Forward is used in connection with Call Forwarding and simply forwards only calls coming from numbers that you choose.

Repeat*Call doesn't have much to do with identifying the caller, but will simply redial a number until you get through, and then call you back when the line is free, allowing you to use the phone for other reasons. Sounds cool, eh? Now you can get through to any radio station you like, right? Wrong. It really isn't as great as it sounds. First of all, it only "redials" for 30 minutes. Also, it really doesn't *dial* the number, but only checks the computer to see if the line is free (and it checks only every 45 seconds). So, it is possible, and happens to me occasionally, that you pick up the phone when the computer calls you back to inform you that the line is free, and you find that it's busy again!)

Return*Call is made for people who just make it out of the shower and to the phone a second after the caller hung up. Boo hoo. In a few keystrokes the call is returned, and the wet, naked person still has no idea what number (s)he returned.

And finally, Tone*Block turns off Call Waiting for individual calls. Pick up the phone, dial *70 and then the number. Voila! No interruptions. But let's say someone calls you. You cannot turn off your Call Waiting in this case, unless of course you also have 3-Way Calling. If you do, you may switch over to the other line and *70 yourself and you'll be fine for the call.

With instant tracing ability soon to sweep the nation, what's the nightmare? Well, basically this hacker's dream is not only for the hacker but for anyone who's got the cash and happens to live in a CLASS infested area. With the public being offered these services, imagine what business customers, or even Sprint/MCI/AT&T are being offered? When ICLID capabilities spread to more states, LCD displays will be showing more and more area codes. Eventually, long distance companies will integrate themselves, and for every telephone connection made, there will be two numbers involved and available to each

end.

When I first got Caller*ID (the service was actually enabled on my line before I received the box) I wanted to learn as much about it as I could. So I played around with it and took it apart. The model that I have (which is relatively old, but there are more ancient ones, too) has a main board inside with some chips and components on it. By ribbon cable it is hooked to an LCD board with LSI chips. There are two buttons (Review and Delete) up front and a battery clip in the back. When the 30th call comes through, it scrolls old ones off to make way for the newest. (This has happened only once to me when I was away for an extended weekend.) What I like about my model is that it will store every call separately. On many models these days, if a call comes through more than once in a row (from the same number), the series of calls will appear under just one entry with a small "RPT" indicator for "repeated call". Personally, I like to know that a certain person called twice a minute for five minutes to get ahold of me, rather than just "Repeat". But that's a personal preference. The flip side is that the extra calls take up space in memory.

The main distributor for ICLIDs is Bell Atlantic Office Supplies (800-523-0552). They sell a few different models. Sears has also been allowed to sell ICLID's through AT&T (who has yet another company making them). Any Sears in New Jersey will sell you one for around $89.95. Radio Shack expects to be offering one soon. That's about it for being able to order them. But there are of course the manufacturers that build these things. Sometimes you can order them directly....

Currently, there are only four manufacturers around that I know of. In Irvine, CA is Sanbar, Inc. (800-373-4122 or 714-727-1911). Sanbar works jointly with another company called Resdel Communications, Inc. I was able to acquire some helpful information through Sanbar and their technical support. Colonial Data Technologies is located somewhere in the depths of Connecticut and makes most of the ICLIDs that Bell Atlantic and Sears/AT&T sell. They aren't too helpful when it comes to questions about Caller*ID, but their number is 800-622-5543. RDI in New Rochelle, NY recently created a smaller company, CIDCO, to produce ICLIDs, as the epytomology of the name might suggest. (I spoke with a fellow there named Bob Diamond. I was pretty embarrassed when, after a few conversations with him, I curiously asked what RDI stood for and found out it meant "Robert Diamond, Inc.") The other manufacturer is a major telephone equipment supplier. Northern Telecom has a massive set of complexes in the southern United States. They make a stand-alone ICLID as well as the only living telephone with a Caller*ID display built in. It's known as the Maestro and can be ordered through Bell Atlantic. It's a simple thing with your basic features such as one-touch dialing, redial, hold, mute, etc.

One thing I aspired to do with my tracer was to try and interface it with my computer. If I could just get the information on the LCD to the serial or joystick port, I could write lots of fun programs. You're sleeping in bed and the phone rings. Unfortunately you're too tired to get up, turn on the light, and see who's calling (actually, CIDCO makes an ICLID with a backlit LCD display). But you left your computer running and within a few milliseconds it announces the person's name, and a Super VGA digitized picture flashes on the screen. Now you know who it is.

And the imagination can run wild with things to do with the computer integrated ICLID: auto-validating BBS's, database management, and so on. So, I called Sanbar (the manufacturer of mine) and talked to one of the head engineers. I asked him if there was any way to leech information from the unit. He said that piping it off the LCD was the best bet, but it might be easier to build a whole ICLID from scratch. After speaking with many people from many different companies, I finally worked on outputting from an LCD. Sanbar used a Sharp LM16255. From Sharp (who were very friendly and helpful) I received literature and specifications. Unfortunately I didn't get too far. Apparently the information is sent in nibbles to the LCD board in parallel format. One must know a bit about electronics and parallel port communications to wire it up.

AND NIGHTMARE

But, fortunately, now there is at least one box available that sends the information via a serial port. (Ah! Such ease.) CIDCO is selling a "business model" that sends the information at 1200,N,8,1 through a serial port in the back. The price? $300. Too much for me. Other companies said they will have similar items, which I expect to be much cheaper.

As far as I know, there aren't many tricks or secrets about using your ICLID at home. When someone calls, either you get their number or you don't; I don't think any electrical modifications will be able to trace untraceable numbers. I hope I am wrong. When I first read the instruction "manual" (leaflet is more like it) I saw that Bell Atlantic had put a piece of tape over a part of the page. I guess they didn't have time to edit the paragraph out. It was in the section of the text showing all the different messages that my box could produce. (It can either show a) a phone number; b) "Out of Area"; or c) a junk number with a few question marks, indicating that there was static on the line or the phone was picked up during the information transmission after the first ring.) Looking at it through the light I saw that another possible message it could produce (and doesn't anymore) was "Private No.". I thought that was great! After speaking with New Jersey Bell, I found out that unlisted numbers are traced along with everything else! Pretty awesome; New Jersey Bell doesn't skimp.

*"All of the latest models of Caller*ID devices are area-code compatible and show your area code where other NPAs will be in the near future."*

If you have Call Waiting, you'll hear the tone, but unfortunately the ICLID won't trace the number. It needs that first ring to "wake it up", so the phone company doesn't bother to send any info. They tell you this in their brochures, but they don't tell you how you can still trace the number of the person who calls you (without going through *57, the main office, and a law enforcement agent). Here is how to do it: When you hear your Call Waiting, tell your friend that you'll call her back and hang up the phone. They will be disconnected and the phone will begin to ring for the person who originally clicked in. Call Waiting leaflets tell you this will happen, but no one tells you what happens next, after that first ring. Voila! Your ICLID will light up and will translate the data that was sent after the first ring. You've traced a call waiting!

As I mentioned earlier, the idea of a per-call block is being thrown around in courts and behind telephone company doors. Supposedly, soon you will be able to make "Private No." show up on your adversary's LCD display when you call. But, it's quite possible now. If you want to call someone and not have your number traced, all you need is a bit of plastic. No "boxes" or equipment. By going through your Sprint/MCI/AT&T Calling Card, the receiver will see an "Out of Area" message. That's what the phone company displays when the incoming call originates through a calling card. Voila! A blocked call. The only drawback is that small surcharge for using the card.

Recently, New Jersey Bell corrected a small computer bug that a bunch of friends and I were having a lot of fun with. When someone called my house collect, the number of their pay phone would show up, so I could reject the call and return it, paying nothing for the connection (assuming the pay phone was a local call). That didn't last for long, and now a collect call brings with it the anonymity of an "Out of Area" message. It was fun while it lasted.

The Network 2000 Saga Continues

EXECUTIVE MESSAGE

Guarding Our Success: Protecting Against UNAUTHORIZED Accounts

By Jim Adams, Executive Vice President

We have the greatest network marketing program in America! Not only are we "the talk" of the network marketing industry, but our program has won high praise from top US Sprint executives who have recently awarded our reaching the one-millionth-installed-customer mark in July. We're proud and excited about this outstanding achievement. NOTHING can keep us from being the biggest, the brightest and the best . . . nothing, that is, *except unauthorized accounts.*

I need your total commitment and help in eliminating this problem. As professionals and protectors of the integrity of our program, you need to make every effort to conquer this challenge NOW!

What Makes an UnAuthorized Account

An account is "unauthorized when the customer claims not to have knowledge of requesting US Sprint long distance service, or claims not to have been informed regarding the details of receiving the service. A customer may be "unauthorized" because the customer:

- do not remember talking to IMR
- thought he or she was getting ONLY the FONCARD℠, when the IMR signed the customer for long distance service, too
- didn't know a fee would be charged to switch from another carrier
- was signed up for US Sprint service by a spouse, who didn't tell the "customer of record" about the change
- customer's signature was forged
- misinformed about 30 free minutes promotion

Correcting Mistakes

Needless to say, it is extremely rare that we find a problem with forged signatures. (*Signing a customer's name on a ballot is against the law, and grounds for immediate termination.)* Most "unauthorized accounts" occur because the IMR was not clear about the details of the ballot.) When an IMR follows the Ron Windham Method of signing customers, there are no such misunderstandings. (Purchase and review the *Wizard of Windham* video, then practice the proper, professional way of getting customers for US Sprint.)

To eliminate "unauthorized accounts" in your organization, we recommend the following:

- Be certain the name on the ballot is the name the phone is currently listed under.
- Be certain the person signing up for the service understands:
  - ✔ They will receive their FONCARD in approximately 30 days.
  - ✔ They will ALSO have their long distance service changed over to US Sprint.
  - ✔ **They will be charged a nominal fee by their local operating company to make the change. (Some IMRs appear to be operating under the misunderstanding that if a person has ALWAYS used AT&T, there is no charge for the customer's first change to another long distance carrier. THIS IS ABSOLUTELY FALSE. Over the past 16 months, I've never had a single person ever change their minds when I told them about the switch charge.)**
- Explain the respective promotion in detail. If they select Dial-1 service, tell them that their 30 free minutes will appear as a credit in their third billing month. If they select Sprint Plus, inform them that they'll receive one month's free long distance (maximum $25) credited on their January 1990 bill.
- The ballot must be signed *by the customer in the presence of the IMR.*
- Give the new customer one of the new flyers immediately after they sign the US Sprint service request ballot. This great sales tool reinforces all the information you told the customer before they signed the ballot. (This flyer is a reinforcement of what you have said. DO NOT use the flyer *in place of* telling the customer this information.)
- Network 2000 has a fail-safe system for discovering unauthorized accounts. A toll-free number is supplied on the back of all US Sprint bills. Using this number, the customer notifies US Sprint that they did not authorize the service. US Sprint then notifies N2K of the situation. And because we have records of all IMRs and their customers, we are able to pinpoint the source of the problem.

What Happens if You Create an Unauthorized Account?

As you know, we are now tracking unauthorized accounts. And we are requiring IMRs who incur these accounts to make an explanation. When unauthorized accounts are found to be the result of IMR neglect or misconduct, disciplinary action (which could include suspension or termination as an IMR) is mandatory.

Again, I congratulate your professionalism. Unauthorized accounts are a threat to our program; we must all work to guarantee they do not occur. Which is why again I say that as protectors of the integrity of our fine program, *you make the difference!*

We've printed stories in the past about Network 2000 signing up people for Sprint's long distance service without the customer's consent. This page from a Network 2000 newsletter shows that they are very aware of the problem.

Nice Telephone Company

October 30, 1990

CABLE & WIRELESS COMMUNICATIONS, INC.
1919 Gallows Road
Vienna, Virginia 22182
(703) 790-5300

Dear Long Island Customer:

We deeply regret any inconvenience caused when your long distance service was interrupted on Monday, October 29. Although we cannot replace the calling time your business lost that day, we want to compensate you for your trouble. Therefore:

> **On Monday, November 5, 1990, between the hours of 9:00 a.m. and 12:00 noon, 100% of your long distance calls will be ABSOLUTELY FREE. That includes instate, interstate, international, 800 and travel calls -- everything!**

Again, we apologize for your inconvenience and appreciate your patience. Thank you for being a valued Cable & Wireless customer.

Sincerely,

Charles J. Gibney
Senior Vice President
for Marketing and Sales

Almost nobody heard about this incident. We weren't even aware of a service disruption! Of course, we didn't get this letter until the 6th, but it's the thought that counts, right?

Nasty Telephone Company

AT&T

Reference: [redacted]

Dear [redacted],

Thank you for applying for the AT&T Universal Card.

We regret that we are unable to grant your request at this time because:

YOUR CREDIT HISTORY INCLUDES DEROGATORY PAYMENT HISTORY
YOUR CREDIT HISTORY INCLUDES SLOW AND/OR PAST DUE PAYMENTS
YOUR APPLICATION INFORMATION DOES NOT MEET OUR PROGRAM REQUIREMENTS

This information was provided by:

TRW CREDIT DATA
36695 12 MILE RD STE 375
FARMINGTON HILLS MI 48018
313-553-8440

If you feel the information is incorrect, we urge you to contact the credit bureau to resolve the issue, and reapply for the AT&T Universal Card.

Of course, if you are an AT&T Calling Card holder, you may continue to use your AT&T Calling Card. Please be assured that AT&T values your continued business.

If you have any questions, please call me toll-free at 1-800-262-5122 between the hours of 8:00 a.m. and 11:00 p.m. (EST), Monday through Friday.

Sincerely,

Pat Dunn
Credit Relationships

In other words, we value your business, but no way are we going to trust you.

an interview with

by Dr. Williams

Recently, I had the pleasure of posing questions to Dr. Dorothy Denning. Dr. Denning has been visible lately to the hacker community.

She participated with Sheldon Zenner in the defense of Craig Neidorf, and has written a paper, "Concerning Hackers Who Break Into Computer Systems". The paper was presented at a conference in Washington D.C., where she also moderated a panel "Hackers: Who are They?", in which Emmanuel Goldstein, Craig Neidorf, Sheldon Zenner, Frank Drake, Katie Hafner, and Gordon Meyer participated.

Dr. Dorothy Denning is well known in the computer security community as author of "Cryptography and Data Security" and numerous research papers. She is past President of the International Association for Cryptologic Research and works in Palo Alto.

This interview was conducted via e-mail over a two-month period.

Many members of the Computer Underground community believe there is a witch hunt afoot against hackers. Buck BloomBecker relates in his book, "Spectacular Computer Crimes" how Kevin Mitnick was harshly prosecuted by officials out to "get the little shit." Operation Sun Devil utilized the efforts of over 150 agents, seizing equipment in 26 locations, but making only 9 arrests, 7 of those computer related.

Finally, even though the prosecutor in Craig Neidorf's trail is to be commended for dropping all charges instead of handing the matter over to the jury, the fact the trial was started and later dropped leads one to believe they too were caught up in the witch hunt mentality before seeing the light. More examples exist. Do you think hackers are being persecuted by law enforcement fueled on by fear and ignorance, or are Computer Underground members not looking past their own bias to accurately judge the current state of affairs?

Let me begin by saying that I am not speaking on behalf of my company.

When I first heard the "witch hunt" analogy, it seemed to make sense.

Most computer crime is committed by insiders, and it seemed like law enforcement was over-reacting to the actual threat posed by hackers.

But as I've dug into some of the cases further and talked with people in law enforcement and industry, I've seen that some of the reports floating around in the computer underground were exaggerated, misleading, and failed to tell the whole story. Some companies have suffered large financial losses because of hackers.

So, the bottom line is that I do not agree that there is a witch hunt, but I can see how people could see it that way. It is true there are more serious problems in this country than that caused by hackers, but this does not mean the damages caused by hackers should be ignored.

Craig Neidorf's trial raises a plethora of questions. At the heart of the issue is why was the trial ever started in the first place.

Even to the casual observer familiar with Phrack, both sets of indictments appeared to be based more on inference than fact. The prosecutor's strongest card was showing the LOD/H was a band of rogue hackers and that Phrack and Craig Neidorf were associated with them, which implies weak evidence on the prosecutor's part. One cannot help but get the feeling Bell South and the Secret Service were pushing hard for this trial - one could suggest pushing past the point of seeking justice. Bell South was embarrassed by the publication of its E911 text document in Phrack and had hidden damaging evidence from the prosecutor. The Secret Service, after expending the efforts of over 150 agents in Operation Sun Devil and claiming a national crackdown on hackers, but making only nine arrests, seemed to be grasping at straws and interested in saving a little face. It is no secret many disapproved of Phrack's content: bomb recipes, password crackers, hacking tips, lock picking suggestions, etc. The philosophizing could go on and on as more points are considered. Why did you think Craig Neidorf was really prosecuted?

I believe that the government prosecuted Neidorf because they thought he had broken the law. I believe that they accepted, perhaps without questioning, Bell South's claim that the E911 document was highly sensitive and proprietary and that a hacker could use it to disrupt 911 service.

What was your motivation to be involved in Craig Neidorf's trail?

I believed he had not broken the law and that I could help with his defense. I was also concerned that a wrongful conviction — a distinct possibility in

a highly technical trial — could have a negative impact on freedom of the press for electronic publications.

Many people feel the government was looking for the first opportunity to send a message that Phrack was not an acceptable publication. Do you speculate this is why the government accepted Bell South's claims without questioning?

While it may be true that the government disapproved of Phrack, I know of no evidence that suggests this was a reason for prosecuting.

I speculate that the government just never considered the possibility that the information they got from Bell South could be wrong and not hold up in court. I hope that in the future they will consult with disinterested experts before deciding whether to pursue an indictment.

Many articles in CU Digest and elsewhere have been critical of current laws governing hackers, viruses, computer usage, information concerning hacking and computer weaknesses, and fraud associated with computers on several grounds. Some laws have been shaped and enacted in crisis more by fear and misunderstanding than truth and good sense. Other laws dangerously erode our civil rights, fail to assign responsibility to computer owners to protect data, dish out harsher penalties to computer crimes over comparative crimes, do not give electronic media the same rights and privileges of printed media, have been motivated more by politics than protections, and in short, are just plain stupid, archaic, and frightening.

What is your opinion of the general worthiness of current laws governing hackers, viruses, computer usage, information concerning hacking and computer weaknesses, and fraud associated with computers?

I am not aware of any computer crime laws that erode civil rights or fail to give electronic media the same rights and privileges of printed media. Also, there are none that I assess as stupid, archaic, or frightening. While many laws may be initiated by a crisis, they generally undergo extensive review, sometimes over a period of several years, before they are adopted. Overall, I'd say the laws are pretty good. As deficiencies are discovered, they get amended and new laws added.

Current laws may provide a means of assigning responsibility to computer owners to protect data. I expect that an individual or company could sue an owner for failing to protect information about them, or failing to provide a promised service because negligent security practices allowed an unauthorized break-in. Nevertheless, I believe it is worthwhile to consider adopting a law where unauthorized entry into a system is at most a misdemeanor if certain standards are not followed and the damage to information on the system is not high. The difficulty is that it may be very hard to set appropriate standards and to determine whether an organization has adhered to them. Currently, it takes several years to evaluate a product according to the Department of Defense Trusted Computer System Evaluation Criteria.

For the most part, the penalties given to persons convicted of computer crimes have seemed reasonable. Although it can be frightening to see someone such as Neidorf facing 65 years in prison, it is fantasy to believe that a judge would assign anything even close to that. Most judges are fair and reasonable; this is why they are trusted with that position. If they assign a penalty that is unfair, public outrage will force them to reduce it. Still, it would be worthwhile to consider establishing a range of offenses with different penalties.

Information concerning hacking and computer fraud is sparse and often misleading. This is a consequence of the fact that the actual evidence in a case cannot be fully disclosed until the case comes to trial.

In addition, companies do not talk about hacker incidents since doing so is perceived to be harmful to business.

Information about computer weaknesses is widely disseminated through conferences, newsletters, professional journals, computer security courses, the CERT, and human networks.

Your paper, "Concerning Hackers Who Break into Computer Systems," states one of the motivations behind hackers is a belief in the free flow of information. Free flow of information has helped propel us to our current heights of technology. Now, hackers point out the disturbing trend of treating information as property instead of the particular way information is expressed. Hackers feel restriction of information will deter learning and hurt the evolutionary process of technology. When information is kept secret behind computer doors, the

result is bad for all of us. As the way Richard Stallman explains the statement in your paper,-"I believe that all generally useful information should be free", do you agree with that point of view?

This is a tough issue on which I have more questions than answers.

On the surface it sounds compelling, at least for certain types of information, and I have always tried to operate from that principle myself by making my research results public. Stallman's arguments against software patents and user interface copyrights are especially convincing. The topic is definitely worth exploring and discussing.

But in any case, I believe it is wrong to use this principle to justify going into a computer system and downloading information to which you are not authorized, or to disseminate information obtained thusly.

One result of secured computers is secured information. What would be your reaction if the results of your research and work were applied to restrict the flow of information in a manner you morally disagree with? Does the effect of computer security on the flow of information ever concerned you?

Computer security per se does not restrict the flow of information. People do. If I want to restrict the flow of some information, I always have the option of not storing it on a computer at all or storing it on an isolated system. Indeed, these methods of handling sensitive data have been a common practice precisely because adequate security mechanisms were not available. The problem with these practices is that they also make it more difficult for people who need to have access to the information to do their work effectively. Computer security gives people the capability to computerize sensitive information and integrate it with other information more easily. This can be a big productivity boost. It makes controlled sharing and distribution of information easier. If I'm on a network that provides a secure cryptographic facility, then I can use the net to send you a highly confidential report without worrying about someone else reading it. By providing mechanisms for controlled sharing, computer security does not restrict the flow of information so much as give you assurance that the information will be disseminated according to your wishes.

Even then, the assurances are weak unless you use mandatory policies for information flow, that is, policies based on classification and clearances and a strict rule forbidding the transfer of information from one security level to a lower one. But most organizations other than the military find mandatory policies too restrictive, and so adopt discretionary ones. With a discretionary policy, it is very hard to control what happens to information once you give anyone access to it. You have to trust that the other people will respect your wishes. Fortunately, most people do, so the lack of assurance may not be a practical problem.

Since I don't want to avoid your ethical question, let me try to outline a scenario that I think gets at it. Suppose that I know of some information that in my assessment will result in harm if it is not freely distributed, but that the person who produced the information is not letting it out. Suppose further that I know the information is stored on some system with a security mechanism that I designed, and that without that mechanism, someone could get access to the information. How would I react? I have never been in a situation like this, so it's hard for me to say for sure what I'd do. I expect I'd go to the person with the information to find out why he or she does not want to give the information out. My own view of the world is extremely small, so there may be some good reasons that I have not thought of. If I am not satisfied with the answer and I know what the information is and not just what it is about, I might consider disseminating the information myself. But, I would have to have very strong reasons for doing this, since the consequences to me or to others could be serious. Another action I might take would be to try to exert public pressure, e.g., by going to the media and reporting that so-and-so is hoarding this information. I might do nothing on the grounds that if the person who produced it had not been there, we would be no better off.

It's been said computer crime costs everybody. However, this statement is often said in glib without much underlying thought. Can you explain if and how computer crime effects everyone in two different examples?

Situation 1: Ten different department stores operate in one region. One store, Store A, is the victim of a computer crime costing a modest amount of its profits for the year. How then is everybody

effected, customers and non-customers? Nothing has happened to the nine other stores, so life is exactly the same for all their customers. Raising prices to make up for the loss by Store A would backlash. In a competitive environment, customers of the victimized store would simply buy the same items priced less at the nine other stores, compounding Store A's losses further. It could be argued the lost money could have been used to pay bigger dividends to stockholders, be used for charitable contributions, increased customer services, etc. In any scenario, counter arguments exist. Only a limited amount of people feel the loss, such as the stockholders, not everybody. If the lost money were to be spread around in a manner that truly touched everyone, the amount per person would be so minute to make its effect wholly ignorable. Finally, there are the doubts that if Store A had never lost the money, it would have been used in a manner that effects everyone in the first place.

Situation 2: A company earns 51.5 million dollars profit one year.

At the end of the year, a hacker breaks into their computers. The total cost to clean up his damage is 0.1 million dollars. How is everybody effected? It is not likely the company will specifically raise its prices next year to make up the lost 0.1 million. Instead, it will probably settle for 51.4 million dollars profit and a tax write off.

Again, the arguments could place the iost money being used for employee benefits, additional R&D efforts, etc. This moves back to the counter arguments of the last paragraph and leaves the question, "How is everybody effected?" Clearly, computer crime is wrong. These arguments are not made as an attempt to justify or lessen the effects of computer crime, but made in hopes of clarifying hard points.

In both situations, you identified the direct financial costs to the companies involved resulting from the crime itself, and then analyzed how these costs are transferred to individuals. In both cases, the costs that reach most individuals seem negligible — unless you're the employee that lost his or her job because of the reduced revenue.

However, the financial costs to the companies can be even greater if publicity about the crime leads to loss of credibility.

When people say that computer crime costs everybody, they are usually referring to indirect costs. The indirect costs include increased tax dollars for law enforcement to fight computer crime, for research and development in computer security, and for government funded organizations such as the National Computer Security Center and the Computer Emergency Response Team. Indirect costs also include expenditures by vendors to develop secure products and by companies for security personnel, products, and training to protect their assets and operations. These costs, which may rise in response to increases in criminal activity, are passed on to customers. In your first situation, all ten department stores may feel compelled to beef up their security, and then raise their prices to absorb the costs.

Similarly, in your second situation, many companies operating on tighter profit margins may respond to a concern for suffering a similar loss by making security enhancements and raising prices.

I should point out that I do not view the above costs as bad, in the same way that I do not view the cost of airport security as bad. As a result of the latter, I can trust that the airplane I board is highly unlikely to be hijacked or blow up from a bomb. Similarly, if I have a secure system, I can trust it to preserve the secrecy and integrity of valuable information assets, and I can be confident that its operation will not be sabotaged.

But, some people say that security places a burden on users. Perhaps an analogy with the Tylenol scare is appropriate. As a result of one incident, it is now a major project just to open a bottle of vitamins!

A consequence of computer crime may be computer surveillance. Because of the widespread concern about break-ins and other forms of computer crime, computer security specialists are developing intrusion detection systems that will monitor systems for break-ins and other forms of abuse. If such systems are not carefully thought out and used, they could result in loss of privacy and degradation of trust in the workplace.

How has the proliferation of workstations changed the needs of computer security?

When workstations were first introduced, many people claimed they would solve the computer security problems of time sharing systems, because users and data would be isolated. In practice, they have introduced at least as many problems as they have solved, because nobody wants an isolated

workstation. One challenge is to protect a workstation from attack by untrusted users and software running on other systems that are connected to the workstation. Sun, for example, recently announced a patch for a security hole in SunView that allowed any remote system to read selected files from a workstation running SunView. Authentication of users, workstations, and software is becoming an increasingly important issue in networked environments in order to make sure that a remote request for service comes from the person or workstation claimed, and to make sure that programs such as login have not been replaced by Trojan horses or contaminated with viruses. A problem that arises with a workstation placed in a public place is how you prevent someone from rebooting the workstation, gaining root privileges, and then causing trouble on that workstation or other systems on the network.

Computer security scientists have developed good computer security procedures, but their record for simply preaching the practice of these developed procedures is less impressive. Today, many computer managers still fail to exercise basic computer security defenses. Can computer security scientists be faulted for failing to impale good security precautions into computer operators, or is that pointing the finger at the wrong person? Everybody plays a part is computer security, but who is most responsible: the user to use basic common sense, the operator to use tools already available, the vendor to develop secure OS's, or scientists to make computers more secure?

Everybody shares the responsibility. Individuals and organizations should look for ways to take greater responsibility rather than for excuses to assign it to others.

Some people in the security industry and system administrators I have had the pleasure of talking to essentially consider hackers to be gum on the bottom of your shoe: They usually get in only when security is weak, are more annoying than dangerous, lack the reason to cause harm but have the ignorance to, and just have the potential to cause an unpleasant mess. While this certainly isn't a glamorous analogy for hackers, would you consider it essentially correct?

It is a nice analogy, but it fails to tell the whole story. Some organizations report considerable losses from hacking and phreaking incidents. To them, hackers are a serious menace.

Do you think BBS's, by their nature, should be regulated as common carriers or as primary publications? Some have suggested regulating BBS's similar to Ham radios and Ham operators. Do you think this suggestion has merit?

Computer bulletin boards have been referred to metaphorically as electronic meeting places where assembly of people is not constrained by time or distance. Public boards are also a form of electronic publication. It would seem, therefore, that they are protected by the Constitution in the same way that public meeting places and non-electronic publications such as newspapers are protected. This, of course, does not necessarily mean they should be free of all controls, just as public meetings are not entirely free of control.

In comparison to the severity of other crimes, hacking still makes relatively big headlines. Hacking's novelty has worn off, so why do you suppose it still continues to captures the press's fancy?

Recent articles have focused more on the constitutional issues raised by the Neidorf and Steve Jackson Games cases.

Your latest area of research concerns hackers. What is your personal motivation or interest to study hackers? Can you give us your answer to the question of your October '90 Washington D.C. conference, "Hackers: Who are They?"

Curiosity and a concern about the growing number of young people committing computer crimes that adversely affect the companies owning the systems they attack. I'm still learning who hackers are. They're all different, of course, while sharing a discourse that is revealed in places like *2600*.

The few I have talked with extensively have been helpful, candid, passionately interested in technology and learning, and ethically conscious and concerned about unethical behavior and the free flow of information in organizations and society. I have enjoyed talking with them. But I would not want to say all hackers are like the ones I've talked with. Many hackers may be unaware or unconcerned about the adverse consequences of their actions on others.

Hackers can be notorious for bragging and shooting off at the mouth, in verbal and in text. From your studies, would you say this is one of the greatest

dorothy denning

reasons leading to their capture and demise? If the characteristics of hackers are homogeneous enough to generalize, what is the typical life cycle of a hacker? Discovery and interest in computers at adolescence, hacker status by high school, in college and in trouble by 21, retired by 22?

Hackers are caught because they perform an act that someone in the company affected by the act assesses is serious enough to investigate, and because there is enough evidence to trace the act to the hacker. Cliff Stoll's book gives a good account of one such case. I haven't talked to enough hackers to know the typical life cycle.

Your husband, Peter Denning, is also a computer security scientist. Do your shared careers ever present interesting situations at home, i.e. stimulating dinner topics, computer religion debates, elaboration of projects, etc.?

Peter is a computer scientist, but security is just one of many areas he's interested in. He is by far my biggest supporter and biggest critic. I mean the latter in a positive way. He goes over all of my papers and offers comments and editorial suggestions. We have lots of interesting discussions, which often lead to new ideas and projects.

For example, the topic of my most recent paper on the Data Encryption Standard came up in a conversation. We never have computer religion debates. I showed Peter my response to this question, and the following dialog took place:

P: When you've been together for 18 years, you don't have many disagreements. You can't even tell where the ideas originate.

D: It has nothing to do with 18 years. We've never disagreed much on computer issues.

P: I completely disagree!

It has been predicted that passive eavesdropping will become the hacking of the 90's. This seems credible as prices in surveillance equipment have dropped over the years. How do you think hacking will change during the next decade?

Well, I don't have any special talents with a crystal ball, but it seems that if the motivation behind hacking is learning about and exploring systems, then I would not expect to see many hackers engaged in passing eavesdropping. Or, is the real motivation to have fun with technology in an illicit way? I expect that there will always be some hackers who try to break through security mechanisms, despite the risks and penalties of getting caught.

Many systems will be practically impenetrable because of improvements in security, but there will be always be systems that are easy to penetrate. As computer security tightens, the attacks may get more sophisticated.

I speculate that there will be more attacks on computers for purposes of espionage, sabotage, or fraud. These attacks will be performed by organized crime, terrorist groups, spies, and individuals out to make a profit illegally. I have heard that organized crime is already trying to enlist hackers, and some hackers may become criminals this way.

You stated your original intent for accepting the Sir Francis Drake interview in W.O.R.M. was the hope of teaching hackers something. Unfortunately, the interview did not move into that direction. What was it you wanted to tell hackers?

The hope was that I might say something so elegant and convincing that it would have the effect of discouraging hackers from breaking into systems. Which reminds me of a wonderful story by Raymond Smullyan in "This Book Needs No Title." Called "Another Sad Story," he describes a man who being overcome with mystical insight, wrote voluminously. When he finished writing, he read his manuscripts over with great pride and joy. Then one day, several years later, he reread his manuscript and could not understand a word of it.

Dorothy Denning can be reached on the Internet at "denning@src.dec.com".

2600 has meetings in New York and San Francisco on the first Friday of every month from 5 pm to 8 pm local time. See page 41 for specific details.

NEW REVELATIONS

by Emmanuel Goldstein

2600 has obtained internal documents detailing BellSouth's future plans for monitoring telephone lines. Their desire is to develop a system more flexible and powerful than that currently allowed by the Dialed Number Recorder (DNR). Its purpose, according to one of the documents, is "to assist our security personal [sic] in identifying intrusions across the telephone network."

What BellSouth is developing here is truly frightening — the ability to spy on any kind of conversation (voice, data, fax) literally at the touch of a button. Add to this the fact that everything obtained will be stored on computers and the potential abuses of this technology shine far brighter than any benefits.

An Overview

The system is to be made up of two separate components: a control unit and a remote unit (used for the actual monitoring). Both of these would be capable of allowing multiple units.

According to BellSouth: "The control unit will be located in a secure area, under the supervision and control of BellSouth Security personnel. This device is to be used to program and control the remote unit(s), gather data, and produce statistics. The telephone network and modem technology is to be the primary means of communications between the remote and control units."

The company is planning to purchase one control unit and four remote units. Each control unit, however, will be able to handle at least 50 remote units. Their long range plans are described as being able to cover up to six metropolitan areas.

Among the features BellSouth described as mandatory was a way of indicating the presence of fax or data communications occurring on the line and presumably capturing them. As for voice communications, the remote unit will be able to "record all analog signals occurring on the targeted number" upon receiving a command from the control unit.

Communications between the two devices are to be encrypted. The monitoring device (remote unit) will be capable of holding the data it captures until the control unit tells it to transfer the information. Doing this will not prevent it from capturing more data at the same time.

Among the information to be exchanged between the two units is an identification code indicating the target number. This code would be translated within the control unit. The company seems especially concerned at not having the actual phone number revealed in any communications. Another piece of data would be a "call sequence number" designed to keep track of the number of communications between the two devices.

Other information includes standard DNR-type data: time the phone was picked up, what numbers were dialed (rotary or pulse), time the phone was hung up. Each single call will be capable of holding 300 digits and dialing *within* a call is also to be time-stamped.

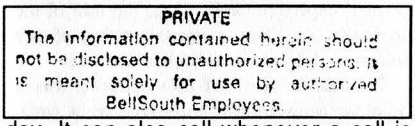
The information on the monitoring device would be held in Random Access Memory (RAM). Also in RAM will be "characterization data" such as the telephone number of the control unit and the alphanumeric unit identification code mentioned above. BellSouth estimates that 64K of RAM will be enough to store data on twenty dialing sessions or 24 hours worth of calls.

Listening In

All of these monitoring devices will be capable of listening to everything on the line, which makes them radically different from DNR's. "When activated," a BellSouth

document reads, "all signals, voice, data, and fax, detected on the target number line are to be passed to the control unit using the communications data link between the remote and control location. The mode of transmission is to be simplex, towards the control unit. The activation of this capability is to be under control of the control unit and will be downloaded to the remote unit at time of activation." The control unit will be able to connect a call from the remote unit directly to a tape recorder. The control unit will also be able to tell the monitoring device to only listen when the phone is off hook or to listen at all times.

The monitoring device is supposed to be able to call the control unit when certain conditions are met, such as the memory being full or at a predetermined time of day. It can also call whenever a call is made from or to the targeted number or whenever a certain *type* of call is initiated, i.e., fax or data. Theoretically, this could also mean calls to a certain area code or to a specific number would enable the remote unit to call home.



Security Features

The two units will be communicating over the regular telephone network via modem, although there will be the ability to communicate in a "private line environment". To prevent unauthorized access, the units will be silent when called. They will only become activated when the right password is entered at the right protocol by the calling device. BellSouth also suggests having "an artificial audible ring" emanate from both of the devices. Communications protocols under consideration appear to be X-modem and AX.25 with a preference for the latter.

Data received by the control unit will require a multi-tasking computer. Operating systems such as OS-2, Unix, and Xenix are being considered. In addition to storing data on a hard disk, tape backups are also likely. Backup control units are also being planned, in case one fails.

As far as physical makeup, each of the remote units, according to one of the documents, will be less than eight inches high, ten inches long, and three inches deep. They will also be capable of running on 60 hertz with internal batteries that will last at least two hours. Both the remote and control units will be capable of future expansion.

The Potentials

Everything seems to indicate that this system is designed for sticking a remote monitoring device in a location *anywhere* between the central office and the target telephone.

You may have already asked yourself a very good question. Why would BellSouth come up with such a system when they could just operate the whole thing out of a central office? Why bother with all of this communication between two units, synchronization, passwords, another phone line, etc.?

Although it was never stated, it appears that this system will be ideal for any agency interested in monitoring certain individuals. Who says the control units have to be located within the phone company at all? It could be anywhere. This kind of monitoring system can operate quite well without the phone company even getting involved.

Under the guise of protecting its system against intrusion, BellSouth is creating a monster. And it now appears that other phone companies around the nation are involved in this as well. The one thing needed for such projects to succeed is continued consumer ignorance.

The following technical synopsis was prepared by the Fraud Division of the U.S. Secret Service and obtained by 2600. While it is stated that this noncopyrighted information is not intended for the news media, it should be noted that it has been rather widely distributed within the industry. We feel our readers and the general public have the right to know the facts in this case, or at least the facts according to the Secret Service. For those that haven't seen it in the papers, the phone company referred to here is GTE.

On February 4, 1989, U.S. Secret Service agents arrested four individuals in Los Angeles and one in Lincoln, Nebraska, for producing counterfeited Automated Teller Machine (ATM) debit cards and for possession of access device-making equipment. When the defendants in Los Angeles were arrested they were in the process of encoding the counterfeit ATM cards with stolen bank account information.

The group was planning to travel to a number of cities throughout the United States to make cash withdrawals from ATMs linked to a specific nationwide ATM network. They made plans to travel in teams to different geographic areas of the country and to use disguises to defeat ATM surveillance cameras, while using each card to its daily maximum for three to five days.

The counterfeit cards were constructed of posterboard cut to the appropriate size and affixed with common magnetic tape. The tape was encoded with stolen cardholder account data on Track 2 for use in ATMs.

Seized concurrent with the arrests were a computer, an encoding device, and thousands of counterfeit ATM cards.

The defendants intended to execute the scheme over a five day period during February, 1989. "Test" cards had been successfully used in at least three cities, which netted the defendants about $5,000.

This case constitutes the first known attack of this magnitude on a major nationwide ATM network.

Bank officials interviewed after the arrests confirmed that the account numbers used in this case would have given the defendants access to the checking accounts, savings accounts, and any lines-of-credit available to the legitimate cardholders. An audit of those accounts revealed this scheme could have netted the defendants as much as five and one-half million dollars had all gone according to plan and had the scheme gone undetected.

One industry expert from outside the bank speculated that it is plausible someone could, using this scheme or one similar to it, access accounts and steal as much as $100 million if carried to the extreme and extended over a 30 day period with careful execution.

In the city where this conspiracy began, several national and regional ATM networks share a single telecommunications carrier which routes transactions between ATMs and banks.

In addition, the telecommunications company, through a subsidiary, maintains a number of ATMs in a proprietary network which they make available on a contractual basis for other networks to use as ATM outlets for their respective cards. Thus, the role of the subsidiary company is similar to that of any bank on the telecommunications network.

The mastermind of this scheme was a computer programmer employed by a well-established software company specializing in the design and implementation of ATM network software. His company was contracted by the telecommunications company to update and expand the existing proprietary network.

The primary defendant's function as a programmer was to implement software which drove ATMs and Point-of-Sale (POS) terminals on the proprietary network in order to make information compatible with, and therefore acceptable to, the main electronic switch maintained for all of the participating networks on the communications system. His position required him to have access to most of the technical data pertaining to software for both the proprietary ATM network as well as the main communications system on which all of the networks were mixed.

In keeping with established industry standards, the telephone carrier subsidiary in this case encrypted the Personal Identification Numbers (PINs) used in conjunction with ATM

cards. This was done prior to transmitting data from the ATM across the proprietary system to the electronic switch where the transaction would be routed to the appropriate bank.

The system targeted in this case is typical of ATM networks found throughout the United States. When a cardholder accesses his account through use of a debit (or credit) card at an ATM machine, the customer is asked to key in his or her Personal Identification Number (PIN). The PIN is encrypted using the universal Data Encryption Standard (DES) method, employing an encryption key known only to the owners of the proprietary system to which that ATM belongs. The account number and other Track 2 data from the ATM card, encrypted PIN, and information about the requested transaction are then transmitted electronically to a switch maintained by a designated communications carrier.

At the electronic switch, messages from several proprietary systems are received and decrypted, using the same DES key as was used to encrypt the data. At that point the information is sorted by the destination bank and encrypted with the proper DES key provided by the destination bank. The transaction is then transmitted across the main communications line to the appropriate bank.

(Theoretically, upon receipt at the bank, the information is once again decrypted using the key supplied to the communications network. However, in practice this step may not actually take place as the recipient bank may elect to accept the encrypted version of the PIN and process it in its encrypted form.)

Upon receipt at the bank, the account is queried and a determination is made relative to authorization or denial of the requested transaction. The flow of information is reversed upon return of a message from the bank to the originating ATM.

To illustrate, if Bank "A" issues ATM cards and maintains their own ATMs at various locations, they are running a proprietary system. A communications carrier must be employed to tie the system together but since there are no other participating banks on the system, the sorting process at the previously described electronic switch need not take place — all transactions are directly between the ATMs and the bank. Even on a closed system such as this, the industry encourages the use of PIN encryption. Furthermore, DES is the preferred standard when PIN encryption is employed.

On the other hand, if Bank "A" elected to enjoy reciprocity with Banks "B" and "C", permitting transactions at all three banks' ATMs, then an electronic switch would be installed to sort and route transactions between all of the ATMs and Banks "A", "B", and "C".

Transactions destined for Banks "B" or "C" from ATMs owned and operated by Bank "A" would still be considered to be on the Bank "A" proprietary system until they reached the electronic switch, where they would be mixed and sorted by the destination bank. At that point, the proprietary ATM networks from Banks "A", "B", and "C" combine to share a common communications carrier, but the networks remain independent and do not share encryption keys. The function of the electronic communications switch is to sort the transactions, determine which encryption key to use and establish how to route the information to the destination.

The system abused in the case in which these arrests were made was similar to that previously described, with the communications carrier subsidiary functioning in the role of Bank "A".

Specifically, the subsidiary owned a network of ATMs and, through a contractual arrangement, accepted debit/credit cards issued by various banks and honored by other networks. When a transaction was requested, the information was handled on the proprietary network until it reached a communications switch where it was decrypted then encrypted with the proper key for the destination bank, and fed into the main communications line used by all of the proprietary systems cooperating in this enterprise.

As a part of their routine business practice, the subsidiary recorded all transactions on the proprietary network before those transactions reached the electronic switch. The intended purpose was to create a transaction log from

which all activities could be reconstructed should a system or other failure occur. The PINs remained encrypted in this recording process.

Either while performing his job, or merely by knowing where to look based on his intimate knowledge of the system, the scheme's mastermind discovered that the key used to encrypt PINs on the proprietary network was a default key, as opposed to a proprietary key selected by network officials. (A default key in an ATM machine encryption device is analogous to a common computer password installed by a mainframe computer manufacturer. Its intended purpose is for testing during the installation phase and it is expected that the default password will be removed once the system is installed and accepted by the buyer).

Upon making this accidental discovery, the programmer realized the value of this information and was able to refer to various software manuals and textbook literature to decipher the key.

The programmer knew data was routinely recorded to the transaction log and that he could access the data transmissions as they were being posted to the transaction log, and thereby "see" all transactions on the proprietary network. It was there, at the transaction log, that he copied account numbers and the encrypted PIN offsets onto his personal computer.

Note: While it is believed the information was copied in "real time", that is, concurrent with it being posted to the transaction log, it could have just as easily been done using another method. The programmer could have electronically copied data from the computer tape containing the transaction log and extracted the same information. Either method would have netted the same result.

At this point the programmer made a conscious decision, according to his post-arrest statement, to use account numbers from only one major bank. He said he did so because he believed that once the crime was discovered, suspicion would center on an internal problem within that bank.

After selecting a generous number of accounts from the targeted bank, the employee wrote a computer program to decrypt the PIN for each of those accounts. He was able to accomplish this using the default DES key. It was later learned that accounts from other banks were also used during the "testing" phase of the scheme and that those accounts and PINs were obtained in the same manner.

He also realized that the network would be reviewed for potential weaknesses once the crime was completed, so he reported the apparent oversight in using the default encryption key on the system and made recommendations to his superiors about how to remedy the situation. The remedies were put in place, ending his access to additional account data. He also accomplished his goal of shoring up the network so that there would be no apparent weakness in the system from which the information could have been obtained.

As an aside, it was noted by the investigating agents that the network in this case had been in operation when purchased by the communications company subsidiary. At the time of this writing it has not been established whether the default key was in use by the company from whom the subsidiary bought the network or whether a proprietary key had been in use.

Next, the defendants constructed counterfeit cards using posterboard cut to ATM card size, to which magnetic tape was mounted. The programmer then wrote a program which he used in conjunction with a magnetic encoding device "borrowed" from his office, to write the account number and other data to each of the counterfeit cards. The data was properly encoded in the appropriate positions on Track 2 of the magnetic stripe.

Among the data elements actually copied to the magnetic stripe were the Primary Account Number (PAN) and the PIN offset.

In systems where the PIN is *assigned* to a customer, the PIN is a direct derivative of the account number and the DES encryption algorithm and is referred to as a "natural" PIN. In systems where the customer *selects* his own PIN, the customer selected PIN would not match the "natural" PIN, so an offset number is

used to resolve the difference. When the offset is added to the customer selected PIN, it will equal the "natural" PIN and the verification is made. Thus, in this case, an offset was necessary as the system was one in which the customers had selected their own PINs.

At the time of their arrests, the defendants were in possession of more than 7,400 account numbers with PINs and PIN offsets, all from the same bank. In fact, as previously mentioned, they were in the process of actually encoding the cards when arrested. Among the items seized during the search and arrest were the programmer's personal computer, an encoding device, and several thousand counterfeit cards in various stages of construction from uncut posterboard stock through finished, encoded cards.

Although a great deal of technology was compromised and used in the execution of this scheme, in the end this crime was one in which a trusted employee exploited his knowledge and position to manipulate and misuse the system.

The only true technical deficiency or error uncovered was that the default key was left in place when the proprietary network was absorbed. Presumably it had been in place since the system was first activated, although that has not been established as fact.

At the time of this writing, it is unknown who should have been responsible for replacing the default key with an active, proprietary key. Perhaps this oversight could have been prevented had a more thorough checklist been used by the communications company subsidiary when they absorbed the system, or by the previous owner of the network. Regardless, had the recognized protocol for securing the respective data been followed, this crime would not have been possible.

Human nature — greed, opportunity, and a willingness by the defendants to commit larceny — combined with human error in not properly installing and reviewing system safeguards account for the forming of this scheme. It is fortunate that the information came to light before the scheme was executed.

The central figure in this case is a high-school graduate and was gainfully employed with a substantial salary. He stated that he was motivated, in part, by his desire to purchase an expensive home and did not want to wait as many years as it would take to save before he could acquire the property he had in mind. His wife is a co-defendant and she too had been gainfully employed with a good salary. Another of the defendants is a graduate of the Air Force Academy and has a Masters degree from a prominent university.

None of the defendants has a criminal record. All have been charged with several counts of violations of Title 18, United States Code, Section 1029, Access Device Fraud. As written, that law provides for substantial penalties. Each count of *producing* or *using* counterfeit cards carries a maximum sentence of 15 years imprisonment and a fine of $50,000. The same penalties apply to the *possession of device-making equipment.* The *possession* of *fifteen or more counterfeit cards* carries a maximum penalty of 10 years imprisonment and a $10,000 fine.

Ultimately, upon conviction of the defendants, the recently implemented Federal Sentencing Guidelines will determine the sentences in this case. Those guidelines take into account the actual and potential fraud losses in white-collar crimes such as this.

At the time of this writing, a superseding indictment is anticipated charging the defendants with multiple counts of 18USC1029.

2600 is always in need of writers!
If you've got a field of expertise or a story to tell, send it in to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953
Questions?
Call (516) 751-2600

DEFEATING

by Lord Thunder

This article should be of interest to those of you who are accustomed to receiving telephone calls by individuals who are not necessarily paying for the calls they make. Oftentimes, these people are called phone phreaks, but most of us know that a calling card does not a phone phreak make. Anyway, you receive an illegal call from someone:

Is it your responsibility to help the telephone company deal with this offender?

Do you keep track of every call you receive, when, and from who?

Should you have to deal with telephone security personnel harassing you?

Of course the answer to all three questions is "NO" and that is what this article is all about.

Let me tell you a story.... From time to time I have been known to receive calls from telephone company security personnel asking me about who may have called me on a particular time and date. However, it seems like I can never remember and find myself unable to answer those questions. This does not mean I do not have fun antagonizing those individuals foolish enough to ask stupid questions. One incident in particular went something like this....

(The names have been changed to protect the innocent.)

R-R-R-I-I-N-N-G-G!

LT: Hello.

TA: This is Ms. Tammy Amesy from Pacific Northwest Bell, and I'm calling to find out who called you from the Portland, Oregon area at 7:43 PM on June 17, 1989.

LT: Lady... I have no idea and if I did, I would not tell you anyway!

TA: What! That person made an illegal call and if you do not tell me who it was I'll have the charges billed to your number.

LT: (Hee Hee... This idiot just screwed up bad!) Oh, ok, who is this again?

TA: Ms. Tammy Amesy of Pacific Northwest Bell.

LT: Why don't you give me your supervisor's name and number and I will speak with her.

TA: (Ah-Ha! I have him scared now [she thinks].) Sure, Lisa Algart at 503-XXX-XXXX.

<CLICK!>

R-R-R-I-I-N-N-G-G

LA: Hello.

LT: Is this Lisa Algart?

LA: Yes. Who is this?

LT: Are you Ms. Amesy's supervisor at Pacific Northwest Bell?

LA: Yes I am. Who am I speaking with?

LT: Hello. My name is Lord Thunder [No I didn't really use my handle]. Did you know that an employee of your company just committed several federal felonies?

LA: Oh my *god!* Please tell me what happened.

LT: (I explain the call to her and told her that Ms. Amesy committed extortion and fraud threats on an interstate communication carrier and also, because she was acting in the capacity as an official representative of Pacific Northwest Bell, she has left her company open to civil and criminal charges for threatening to reverse

TRAP TRACING

charges in order to illegally extort information from me, and I was planning on calling the Federal Communications Commission (FCC), the Public Utilities Commission (PUC), and the Federal Bureau of Investigation (FBI) to press charges.)

LA: Please, I'll talk to Ms. Amesy and make sure nothing like this ever happens again.

LT: OK, but I want something. I want a signed letter of apology from Ms. Amesy on Pacific Northwest Bell stationery.

Two days later I received the letter on Pacific Northwest Bell stationery:

"In reference to our conversation on June 23, 1989 regarding calls made to your telephone number, I apologize if you felt inconvenienced or offended. Please fell free to call if you have any questions.

Sincerely,

Ms. Tammy Amesy

Service Representative"

Now that was just one example of an attempt by the phone companies to perform trap tracing. I think code abuse is juvenile to begin with, but I do have a few things to point out on both ends.

1. Do not call someone illegally who is going to screw up and mention your name when the telephone company calls to check it out.

2. The telephone company only checks into the lengthy calls on bills with excessive costs. Keep your calls to a minimum of numbers and length to avoid being looked into.

3. Do not call relatives or personal friends that are not involved with phreaking with illegally obtained codes.

A few other things to mention. Some of the companies, like U.S. Sprint are more likely to call you up just to verify that you do not know the actual card holder. This is their way of making sure that the calls that the cardholder says are not his really are not his. I have been contacted by some of the companies (U.S. Sprint among them) a full six months after the calls were placed to answer these types of questions.

I had another interesting incident with a lady known as Julie of TMC. Some of you might remember her from a few years back. Anyway, I had been talking with a friend of mine for 45 minutes or so on a Thursday evening and on Friday afternoon I received a call from TMC Security demanding to know who I spoke with for 45 minutes the night previous. I was not about to tell them what they wanted, but it still was a little difficult to not remember who I spoke with the night before.

I whipped up a story about running an anonymous login in AE line or something. It lacked a little imagination, but it worked. Another idea you might want to try is say that you have one of those long play answering machines that does not turn off until the caller stops talking. Then mention that you had some long obscene call on there that filled up most of the tape and you wished you could find out who it was too.

So that is all I have to say about trap tracing. If you must use codes or calling cards illegally to call people, at least know how to protect yourself from security by letting your friends know what not to say when these people call to inquire.

write us

Questions

Dear 2600:

Being a new subscriber, I was wondering what the 2600 represents in the title of your magazine?

Snoopy

2600 hertz at one time was a liberating cry used by phone phreaks. By sending a 2600 hertz tone down the line when connected to a long distance number, the number would disconnect and you would have total control over the long distance trunk. Not only that but billing was bypassed. This was commonly known as blue boxing. These days that method rarely works, but of course there are many others.

Dear 2600:

What steps do you take to preserve your mailing and contact list from the authorities? Is the list encrypted? Furthermore, how do you ensure against infiltration? Not that I'm the paranoid type, but this is really something you should be considering, as I'm sure the paranoid government services would be dying to get ahold of your mailing list. As a service to your clients and contacts, please keep this information secure.

There is a mail network in the works up here. I'm sure we can make arrangements for access to it as soon as a few minor security arrangements are worked out. The international flavor of this network, I am sure, as well as its constant flexibility will make it one of the most elusive and one of the most difficult to pin down from a legal perspective. I look forward to having it as one of the ways of protecting Canadian rights under the charter, and American rights under the First Amendment. Like a multinational company, this network would build capital in one of the most fundamental resources: the international protection of free speech.

JB
Ontario

Freedom of speech is not protected by hiding from the authorities. If you're trying to protect rights, then be as open about it as you can. If more people were willing to do this, we wouldn't have to be afraid.

Regarding our mailing list, don't worry. We wish we could say more, but if we did we'd be giving out the information that you want to remain confidential. We don't see infiltration as a problem. It is a two-way street, after all.

Dear 2600:

I am new to phone hacking. I sent away for plans to build a blue box (the plans they sent me are for the latest version supposedly). The box uses two 8038 intersil function generators and a 741 CV OP Amp. It has 10 25K trim pots used to tune the pole switches for the keys 1-9, KP, ST, and 2600. (The plans came from Alternative Inphormation, PO Box 4, Carthage, TX, 75633.)

Well, now that I have the thing nearly completed, one of my friends tells me that the blue box is not safe to use. He says he has heard that the phone company has equipment that can instantly pick up on the blue box and that they can get someone out to your house in minutes. This sounds like total bull to me. I was wondering if you guys knew whether or not the phone company can pick up these things that fast or not.

Confused in Kentucky

If they really wanted to, they could. But we doubt in this day and age they would really care. Unless you're from one of those rare places where blue boxing is still a problem for the phone company. Of course, if you're doing anything controversial on the phone, using your own line is not a good move.

Dear 2600:

A few weeks back I came across a number for a system in the U.S. but I can't work out how to use it.

After calling the number (1200 baud), you get nothing on your screen until you press the return key, then you are given a line saying "YALE ASCII TERMINAL COMMUNICATIONS SYSTEM v2.1" and a menu with which you select your terminal type. After this you get nothing except one line of text giving you a number to dial in the U.S. for help.

If you or any 2600 readers know anything about this system, can you please try to help with commands, etc.?

Ashley
U.K.

We suggest calling the number for help. Why not?

Information

Dear 2600:

Regarding the schematic for a device that

a letter

would display a digital readout of a string of touch tones applied to its input: PI-COMMunications at 8455 Commerce Ave., San Diego, CA 92121 sells a DTMF decoder with an LED readout. It will decode all 16 touch tones. It is made to plug into the speaker output of a ham transceiver and a remote speaker can be plugged into it so the user does not lose the audio. It can be used on the telephone by modifying an old acoustical modem coupler to do what the writer wanted. The company is also working on a similar device that will have a ten digit readout with two memories, but I don't know if that is available yet. I think they sell the above device for $130 but you will have to contact them to find out.

Roy

Dear 2600:

I've read some articles about scanning for calls and want to add some information about doing so in Germany. We actually have three different car phone systems and a cordless phone system.

Carphone system B1 is frequency modulated and uses channels 1-37. Car frequencies: 148.410-149.130 Mhz. Exchange: 153.010-153.730 Mhz. Channels are in steps of 20 Khz.

Carphone system B2 is frequency modulated and uses channels 50-86. Car frequencies: 157.610-158.330 Mhz. Exchange: 162.210-162.930 Mhz. Channels are in steps of 20 Khz.

Carphone system C is cellular and has 222 channels. Car frequencies: 451.3-455.74 Mhz. Exchange: 461.3-465.74 Mhz. Channels are in steps of 20 Khz.

Carphone system D is planned for the future. It'll be in the 900 Mhz range.

Cordless phones use channels 1-40 with base frequencies of 914.013-914.988 Mhz and handset frequencies of 959.013-959.988 Mhz. Channels are in steps of 25 Khz. This system is known as Sirus.

There is also a service called TeleKarte, a German equivalent of the phone card. On the card is a microprocessor, which has stored your credit card number and a personal ID number that can be changed by the owner whenever he wants. If the owner is on a trip in the USA, he can take part in a service called "Deutschland Direct" (Germany Direct). He can call the German operator at Frankfurt toll-free under the number 800-292-0049. The operator will then ask his card number, name, credit card number, and the number to call in Germany. All costs of the call will then be charged to his credit card.

S.D.

Dear 2600:

An often overlooked place for telephone experimenters to poke around is the 811 prefix (in California). This prefix, which is used by the BOC's, holds much more than the local billing office number. From my Pacific Bell location in California I have found telco office numbers, test numbers, computers, and other things that I haven't figured out yet. Here's a sampling: 811-0317: "Testing 1234" recording; 811-0428: Pac Bell retiree services; 811-0460: computer tone; 811-1000: computer tone; 811-1212: voice computer, answers with "hello", requires numbers and access code entered by DTMF; 811-2060: computer tone; 811-298x: dead line for 10 minutes; x is 0-9; 811-3091: Pac Bell security; 811-4444: Pac Bell employee newsline recording; 811-707x: same as 298x. If you have the patience, scan all numbers in the prefix. You may want to scan during non-business hours because lots of the numbers use answering machines. These machines often identify what the number is used for. All calls to the 811 prefix are free, and many numbers are dialable from throughout the state. Happy hunting.

Mr. Upsetter

Just about every phone company outside California seems to block calls to those numbers. We do know ITT allows calls to those numbers in the 213 area code, among others. The other companies probably don't allow it because the 811 exchange doesn't look right. You can reach the numbers by using the ITT carrier access code (10488) plus the number or using the ITT calling card (950-0488). But expect to pay for a long distance call to that region. By the way, ITT is the only company we know of that provides nationwide 950 access without a surcharge. We highly recommend it and hope the other companies wake up to this valuable service.

Dear 2600:

An interesting service I just heard about: 1-900-STOPPER. $2 per minute local, $5 per minute long distance. You call it, then touch tone in the number you really want to call. Voila! You can't be caller-ID'ed, as the call now originates from 1-900-STOPPER.

drop your letter

Fascinating to see how this caller ID war is shaping up.

EH

It's another rip-off that preys on people's fears. But it won't allow you to call 800 numbers, many of which have bypassed this entire caller ID debate by just doing it anyway. It's got a different name, but for all intents and purposes, nationwide caller ID is being used by a select few!

Dear 2600:

I found an interesting phone number at 212-571-3675. It seems to be a private company phone line verification and feature access point. It uses a synthesized voice to repeat back the phone number you touch tone into it.

D

That computer was floating around as a New York Telephone test number a couple of years back. Apparently the testing is over and the service is being used. We're sure it does more than repeat back the number you give it. The question is what?

Information Needed

Dear 2600:

I am writing a book about hackers and their history. As part of my research, I would like to hear from these people or people who can put me in touch with them if they are interested: Al Bell, Jim Phelps, and Tom Edison (former TAP editors), Fred Steinbeck, Bill Landreth, Joe Engressia, Kevin Mitnick, John Drake, Frank Drake, Castaalia, Aiken Drum, Midnight Owl, John Steen, Spartacus, Nick Sade, Crimson Death, Doc Telecom, Shadowhawk, Laser, The Prophet, Tom Anderson (friend of Bill Landreth), Herbert D. Zinn Jr., Lex Luthor, Knight Lightning, Erik Bloodaxe, The Mentor, Time Lord, Blade Runner, The Leftist, Adelaide, Phiber Optik, King Blotto, Phrozen Ghost, Lone Wolf, Little Silence, Captain Quieg, Unknown Warrior, Lee Felsenstein, Richard Greenblatt, Bill Gosper, Stew Nelson, Jack Kranyak, Jack Cole (the last two former editors of TEL), and any other high caliber hackers and phreaks, especially those who were active in the 70's and 80's. They know who they are! I am also interested in obtaining literature from these organizations and hearing from people associated with them: Chaos Computer Club, Phrack, Legion of Doom, and any other semi-organized group of hackers. Lastly, I would like to obtain any issues of these short-lived hacking magazines: Reality Hackers, W.O.R.M., Computel, PCC (People's Computer Company), Technology Illustrated, Journal of Community Communication, Altair User's Newsletter, Micro-8 Newsletter, Silicon Gulch Gazette, Bell System Technical Journal (years 1956, 57, 60, and 61), Syndicate Reports, and Carolina Plain Dealer. Any other information or literature which could be useful would be appreciated. I am willing to trade or purchase useful literature. Write to: Dr. Williams, PO Box 5314, Everett, WA 98206.

Complaint/Response

Dear 2600:

I am writing this letter to inform the other readers of 2600 to beware of an ad that has been running in the 2600 Marketplace for several years now. The ad I am referring to is the one that advertises TAP back issues for $100. The ad has used several names over the years such as "P.E.I." and currently is using "Pete G." The address is PO Box 463, Mt. Laurel, NJ 08054. P.E.I. or Pete G. states that "he is the original" when it comes to TAP back issues, complete with "schematics and special reports". I ordered the complete set from him awhile back for $100 and I feel I was ripped off! What Mr. Pete G. does NOT tell you is that he reduces the two inside pages of most of the issues down on the photocopier so they will fit on ONE 8 1/2 x 11 sheet of paper! I feel that I am justified in saying that about 60-75 percent of the material is NOT READABLE! It would take someone with 20/20 vision and an electron microscope to even attempt to read some of the pages! Issue #50 of TAP was a special double issue and he reduced it down on the copier and the print is not legible on about 50 percent of that issue! The so-called "special reports" he refers to in his ad are nothing more than a couple of reprints that appeared in the previous issues. I feel that anyone can charge what they want for what they have to sell, but I sure think one should be informed as to what he is actually buying also.

Rainbow Warrior

Pete G. replies: After extensive investigation, we cannot identify the Rainbow Warrior nor locate any record of a sale to him within the past two years. Therefore we will address his complaints

in the mail

individually.

First of all, Pete G. is and always has been me. We began advertising in the very first 2600 issue that took advertising and have been in every issue since. Purchasers were instructed to make checks and money orders payable to PEI only as a convenience so they would not have to send cash. PEI is a corporate entity which can process their checks.

Since the balance of his complaints address the quality of the copies, let me state that I have an original set which I received as a subscriber. The first issue was mimeographed in 1971 and the quality of the issues did not improve for many years. Our copies are professionally prepared. Each page is individually set for tone, size, and layout from an ORIGINAL. We cannot improve upon the existing copy, only reproduce it as faithfully as possible.

Many persons purchased copies of my TAP sets and in the following months ran ads in 2600 offering copies of my copies for other amounts of money. NONE are still advertising. It is a very time consuming and labor intensive business to prepare these copies. We are still going strong.

In closing I might add that Mr. Warrior received as the first page of his order a notice explaining our satisfaction policy and offering to replace any pages he was dissatisfied with. He NEVER advised us of any dissatisfaction with the product.

If anyone has a problem with an advertiser, please try to resolve the problem first. If you receive no satisfaction, then come to us. We will continue to run Pete G.'s ads as we see no evidence of wrongdoing.

The COCOT Article

Dear 2600:

I just received my first issue of 2600 Magazine and loved every page of it. Of particular interest was the article on COCOT's by The Plague. The article was very informative and very timely, as those vile COCOT's have started to pop up in this area in unbelievable numbers. I have a few additional ideas to add. First, instead of using the call forwarding to forward all calls to your number, why not make the COCOT forward all calls to a long distance computer? The COCOT is local to you and it gets nailed for the calls.

Another idea is to confuse the average owner of a COCOT that allows remote mode. Forward the calls from one unit to another COCOT. When the owner calls the first unit, he gets the second unit, and if done to enough of his COCOT's, it is bound to drive him nuts. My final suggestion regarding COCOT's should only be inflicted on those COCOT's that are really vicious about ripping people off. It requires the help of a friend in another part of the country who also has been the victim of a vicious COCOT. Forward all calls from local COCOT A to distant COCOT A. Then have your friend forward distant COCOT A to local RBOC phone A. Now, get an unrestricted dialtone on local COCOT B and call local COCOT A. The call will forward to the distant number, which will forward to the RBOC phone local to you. Leave COCOT B off the hook and go and answer local RBOC A. Now leave that one off the hook also. Both the local and distant offending COCOT's are racking up a large bill, and will continue to do so until some moron comes by and hangs one up. If you wanted, you could get the unrestricted dialtone on local COCOT A and place the call to the distant COCOT from there, but then you haven't screwed up as many phones as possible.

I guess if you were particularly nasty and have a lot of friends who can get their local COCOT's to get call forwarding, you could run up bills on a bunch of phones by making them all call each other. Neat, huh?

I'd like to reply to a letter written to 2600 in the same issue from Jeff. There are several ways to listen in on cellular telephone conversations. The easiest would be to buy a scanner and modify it to pick up the cel frequencies. However, if you don't want to invest in a scanner, or don't know how to make the necessary modifications, here is a neat little trick for listening in on local cel calls.

It requires two televisions with separate antennas hooked up to each UHF terminal. Put one tv on top or next to the other (on top seems to work better, but isn't always practical) and tune them both in the channel range of 75-83. Turn off the sound on one. Try different channel combinations until you find a combination which produces a different static pattern than the other combinations. You'll know when you see it. Now use the fine tuning on the one with the sound off until you hear a break in the static

on the other tv. You are now in the correct area for picking up cel calls. The fine tuning will let you switch between the various cel frequencies. In my area I tune the tv with the sound off to 75 and the one with the sound on to 83. You will have to fool around with it for a while to get it to work, but once you find the proper setup, you are set forever. This little trick is why the FCC is requiring all new tv's to only go up to 74.

Halo Jones

Dear 2600:

I am writing to thank you for your excellent article on COCOT's. I am glad that someone finally told how it really is.

Recently I was a victim of a collect call placed from a COCOT. I was charged close to thirty dollars for a 10 minute call. The offending company was "Operator Assistance Network". I quickly called my local phone company and had the charges deleted. But I'm sure many other people who get victimized by such rip-offs don't do anything about it.

Taking the suggestion from the article's author (The Plague), a group of friends and myself have formed a neighborhood patrol called C.O.P. (COCOT Obliteration Patrol). By the name, I'm sure you can figure out what we do. To date we have eliminated about 65 COCOT's, and only three of those have been repaired. We prefer to "behead" the COCOT's by removing the handset, thus innocent people are NOT ripped off by dropping money into an otherwise dead phone. Our neighborhood is now almost free of these evil phones and C.O.P. will not rest until all COCOT's are out of commission.

Dan
Denver, CO

This isn't quite the way to go about it. All COCOT's are not necessarily bad. To assume they are is to write off an entire branch of technology because of a few bad experiences. Ripoffs should be eliminated. But COCOT's can actually do some good if they improve upon the service already available. It's up to us to see that they do.

Dear 2600:

You've been duped! Your article in your Summer 1990 issue entitled An Introduction to COCOT's was either (a) written by a representative of one of the local exchange carriers or (b) your writer (The Plague) has been receiving some awfully poor information regarding the pay telephone industry.

The real pay telephone rip-offs are not the independent pay telephone companies, most of which are small, independent businesspeople such as ourselves. The real rip-offs are the major local exchange carriers who subsidize their pay telephone operations with regular telephone revenues. Every one of us pays extra in the form of higher local telephone bills to support the L.E.C.'s inefficient, unresponsive pay telephone bureaucracy. Why should your home and business telephone charges support your L.E.C.'s operations?

This is not to say that there haven't been abuses in our industry. But the vast majority of us deserve better than you've shown us. Your article plays right into the monopolistic L.E.C.'s hands, who would like nothing better than to eliminate all competition and return to the days of total uncontrolled monopoly.

R.S. Grucz
Executive Vice President
American Public
Telephone Corporation

It only takes a few rip-off COCOT's to give the entire industry a bad name. We think it's important to clearly label those companies that are engaged in ripping off the public. You should do the same and disavow yourself of those companies. There need to be some basic standards introduced (equal access, 950 access, clear rate structure, etc.). We hope to hear more from your perspective and we encourage our readers to tell us if they've had any positive experiences with COCOT's and AOS companies.

Dear 2600:

I have been a subscriber for the past several years and would like to congratulate you on a fine publication. Although I do not agree with your position on several subjects, I am glad that there is a responsible forum for these ideas to be expressed. I also applaud the fact that you print dissenting views. Your summer issue which has a large section on "Negative Feedback" illustrates what I am talking about.

I am as against the abuse of power by some government agencies and the predatory, if not illegal, acts by some public companies as you are. However, I believe that these acts do not justify illegal acts by individuals. Your publishing accounts of these abuses is the best way to better the

situation. The malicious and illegal acts of some individuals only helps the government justify their abuses and makes things worse.

The article, An Introduction to COCOT's, describes and endorses actions which I deplore, but as I stated above I am glad that there is a place where such articles can be published. One comment that I would like to make is that the justification which the author claims for his thesis is greatly eroded by his hiding behind a fictitious name. If he thinks that his position is morally correct, he should follow the path of other contrarians by using his own name.

Guyler Magruder
Singapore

Prison Phones

Dear 2600:

If you want a caller ID ANI system, Nuts & Bolts, PO Box 1111, Placentis, CA 92670, for around $69.95 has one but it only works in areas with Caller ID. Anyone wanting a high speed DTMF monitor can buy one from Contact East at (508) 682-2000 for around $280 along with neat toys like lineman test sets, tone test sets, line aid inductive amps for tracing, and a lot more. Granted, this stuff is not cheap but remember this is the REAL thing.

As far as phreaking from inside prison, it can be done but only on non-AT&T phones. We have collect-only here, but I got around them as follows. Ours has a recording that asks you your name. When the party you are calling answers, it plays the recording and tells you to press three to accept the call. To start with, I dialed a number to a recorded message like the one at our helpful AT&T office (ha). The recording triggers the phone to accept the call. You don't state your name when asked, but bypass it by pressing a number on the keypad until the call is placed. As the call is accepted, you'll hear the recording say "Thank you for using XXX." As soon as you hear the click that kicks in the recording, you press the receiver level down for about 30 to 50 milliseconds to hang up the switching network. You'll hear the unrestricted dial tone under the finish of the thank you message. You quickly hit the 0 once for local and twice for long distance. When talking to either operator, you simply ask to be connected to a particular number because your call is not going through. Keep it simple to avoid suspicion.

C. Rebel

We left out your location because we assume you want to continue using this.

Privacy Preservation

Dear 2600:

Reading about the Secret Service's witchhunt gives urgency to the need to deal with the increasing government rage for total manipulation of people's lives, and the need for people involved in anything controversial to try to protect their privacy. The government's passion for prying into one's privacy has reached the point where one getting "controversial" mail should consider getting a mail drop. One's mail is sent to the mail drop's address and is mailed to the customer's address by the mail drop operator. Finding a mail drop that is well run, and reasonably priced can take time, but they are out there. Many of them seem to feel they are entitled to large amounts of money for cruddy service, judging from the nearly illegibly scrawled replies I've received from a number of them.

One of the best sources for mail drops is Loompanics' Directory of U.S. Mail Drops for $12.95, which is well worth the price. Loompanics' address is PO Box 1197, Port Townsend, WA 98368. They send books via UPS.

The government has adopted the stance, and the public seems to have come to believe, that the government has an inherent right to keep track of one from birth to death, and that if someone is able to "fall through the cracks", that is itself a wrong to "society", and that if only the government can keep better track of people, it can make things "the way they are supposed to be".

The ability for people to change their name existed long before the social security number came to be used as a de facto name to track people through their lives, and the right to change one's name was expressly meant to enable one to make a break with a past phase of life, or informational detritus stored on one by various entities.

Here in California, the courts have ruled that one has a right to change one's name without court process, and that court process is entirely parallel, simply to make the change a matter of official record. One can go down to any state motor vehicles department and have one's name changed simply by filling out a small piece of paper

for a name change of one's state ID card or driver's license. However, I've found out that one's old name is stored on the state computer for retrieval whenever one is stopped by fuzz. The DMV also takes one's thumb print for a license or state ID card.

Reverend Doktor
Norman Appleton

Wiretap Clarification

Dear 2600:

Reference is made to Hunting for Wiretaps, a letter to the editor which appears on page 24 of the Summer 1990 issue of 2600.

Although I have no quarrel with his observation that the phone company is the wrong place to shop for a service that can locate wiretaps, a number of other comments made by the author of that letter cry out to be corrected:

1. He asserts that series taps are the only kind of tap used by the phone company. The most common type of transitory tap there is takes place when a telephone lineman hooks onto your line using his handset. When he does that he has two choices: TALK and MONITOR. In the TALK mode the handset is connected in parallel across the line and works pretty much like any other extension. You can talk and listen and you draw current. In the MONITOR mode you are using a capacitive tap wired in parallel across the line. You can hear because the voices of those speaking act as AC and are passed by the capacitor. No current is drawn. We are dealing with a high impedance parallel tap, not a series tap as the writer suggests. There are several other ways that bridged (parallel) taps are used. Some are hostile and others are the result of the phone company building mirror image MULTIPLES into the system ostensibly to allow for future expansion in one or another direction. What this means is that if you listen to the correct pair on the frame in your building, you can hear your neighbor's conversations and in a like manner one of your neighbors may well have a tap of your phone mounted on the frame in his building. These parallel taps were built in by the telco to give them more flexibility in assigning lines. This sort of configuration isn't always there, but it is fairly common.

2. The author talks about 12 volts on the phone lines. He should know that the voltage found on the phone lines, unless an off hook phone or tap draws it down, is between 48 and 52 volts throughout the country.

3. The author advises the reader to "put your hand on the cable and follow it out." This "procedure" suggests that the author either lives out in a tent in the middle of a desert, miles from anyone else getting phone service, or that he has never performed the service he describes. If he has a normal house or office, not too far from his telephone is a wall through which phone wires run. How, short of demolishing the premises, does he propose to put his hand on the cable and follow it out? And how does he expect to use this procedure at the intermediate distribution frame where many wires cannot be seen or grabbed without disconnecting hundreds of phones belonging to other subscribers? How does he follow his cable through a gas pressurized splice in a manhole? Assuming he had the expertise to open such a splice without demolishing it, how does he even know that he is in the right manhole, or which of the several huge black cables entering this vault through underground conduits, contains the cable pair that go to his phone?

The business of climbing the poles is also unworkable. Many of the splices are fed by two or three cables containing hundreds of pairs of phone lines each. How does he plan to figure out which cable to hold onto? Most splices are sealed and weatherproofed. How, without demolishing the splices does he plan to get in and inspect them and follow his own phone line out? Many of the splices are located many feet from the telephone pole. Does he plan on going hand over hand along the huge black cable and dismantling the sealed splice with one hand as he holds on with the other? And what happens when he comes to a block box mounted on the ground or on a pole? Assuming he has the special key and a can wrench to open these, which of the hundreds of hidden prewired terminations go to his phone as it enters this panel and which of the hundreds of identical orange and white jumpers go to his service as it leaves the panel?

The author says that "the best solution is to have the phone disconnected and not use it at all." After going through all that work to see if his line was clean, who could blame him for switching to signal mirrors and tom-toms?

middle island, n.y.

Certainly it is possible to conduct a competent sweep of the phone lines for taps, but not by using the procedures outlined by the author. In fact, the procedures he outlines virtually assure the would-be wiretapper that he will never get caught.

Alan M. Kaplan
Attorneys' Investigative Consultants
Las Vegas

A Modern Proposal

Dear 2600:

Having received your Spring 1990 issue, I immediately perused it. The articles on the harassment, arrests, etc. of hackers and phreaks disturbed me.

Because of this, I would like to put forth a proposal for debate within this magazine. In Irwin Strauss's book "How To Start Your Own Country", a small country known as Sealand is cited. Sealand is located near the mouth of the river Orwell in the English Channel. Pirate broadcaster Paddy Roy Bates laid claim to some WW2 vintage gun towers, which are very similar to offshore oil platforms. I believe it would be possible, with backing, to purchase either a boat, ideally a decommissioned oil tanker, or an older offshore oil rig, anchor it in a relatively protected area in international waters, say, in an unclaimed atoll or some such. It could then be used as a hacker/data haven, or a hacker freeport.

If there is enough interest, I may attempt this in the future.

Dr. Deviant

We had some pirate radio people try this near us a few years ago. They were in international waters, but they still got nabbed. The sad fact is that the U.S. government can and will go anywhere to stop you if they feel they have to. But there's nothing wrong with trying it anyway.

Neidorf Defense Fund

Dear 2600:

I enjoyed reading your interview with Craig Neidorf in the summer edition of 2600. I was also dismayed when I read that the EFF was not planning on funding his defense. For some reason, I had thought that defending people against governmental abuse was what the EFF was all about.

I was also disappointed that 2600 did not publish the address of the Craig Neidorf Defense Fund. I, for one, would like to send the guy a check to help him with his attorney fees. There are a few others in the BBS community out here on the West Coast who would like to help.

Jeff Hunter and
The Temple of the
Screaming Electron

We hate to disagree with our readers but we did print the address on page 40. Here it is again: Neidorf Defense Fund, Katten, Muchin, and Zavis, 525 West Monroe St., #1600, Chicago, IL 60606-3693, Attn: Sheldon Zenner. So far, contributions from our readers have been pretty dismal. If you made a contribution and you didn't get a personal thank you from Craig, let us know. If you'd rather make the donation through us, we'll be happy to forward it to him. But please do what you can as this battle is being fought for all of us.

Which Decoder Chip?

Dear 2600:

I enjoyed the Spring 1990 issue immensely. The DTMF decoder project was just what the doctor ordered. Would a more commonly available CD22204E tone decoder chip be a good substitute for the SSI202? The physical pinout is different but it seems to be electrically equivalent. For another excellent source of electronic parts, get a catalog from Circuit Specialists, PO Box 3047, Scottsdale, AZ 85271-3041.

Finally, here's a COCOT number to try: 216-928-6790. After two or three rings it answers with a female computer voice saying "thank you" followed by four touch tones.

Akron, Ohio

We're told the SSI202 is available at Radio Shack. You can't get more commonly available than that. Try these COCOT's at 212-268-7538 and 212-268-6129. Hitting a 0 will turn on a microphone and allow you to hear street noise in New York City. Or maybe a drug deal on the neighboring phone.

General Observations

Dear 2600:

For my fellow readers' info it might be important to know that beige boxes are still very available at airports. The courtesy phones that summon local motels, rental car companies, etc. are more courteous than one would imagine. The best protection I've found so far is a small speed dial box under the set connected with a simple modular

(continued on page 40)

CONVERTING A TONE DIALER

by Noah Clayton

A very simple modification to Radio Shack pocket tone dialer part #43-141 ($24.95) can make it into a red box. The modification consists of changing the crystal frequency used to generate the microprocessor's timing. To make this modification you will need a Phillips screwdriver, a flat bladed screwdriver, a soldering iron, a pair of long nose pliers, a pair of wire cutters and a 6.5536 MHz (megahertz) crystal.

Orient the dialer with the keypad down and the speaker at the top. Remove the battery compartment cover (and any batteries) to expose two screws. Remove these two screws and the two on the top of the dialer near the speaker. There are four plastic clips that are now holding the two halves of the dialer together. Push on the two bottom clips near the battery compartment and pull up to separate the bottom part. Now slide a flat screwdriver into the seam on the left starting from the bottom and moving towards the top. (You may have to do this on the right side as well.)

When the two halves separate, slide the speaker half underneath the other half while being careful not to break the wires connecting the two. Locate the cylindrical metallic can (it's about half an inch long and an eighth of an inch in diameter) and pull it away from the circuit board to break the glue that holds it in place. Unsolder this can, which is a 3.579545 MHz crystal, from the circuit board.

The hard part of this modification is getting the new crystal to fit properly. Bend the three disk capacitors over, as indicated on the diagram, so that there will be room for the new crystal. Also remove the indicated screw. Since the 6.5536 MHz crystal you have is probably much bigger than the crystal you are replacing, you will need to bend the leads on the new crystal so that they will match up with the pads on the circuit board. Place the new crystal on the circuit board using the diagram as a guide. Solder the new crystal in place. As an added touch you might peel the QC sticker off of the PC board and place it on top of the crystal. Now carefully snap the two halves back together while checking to make sure that none of the wires are getting pinched or are in the way of the screw holes. Put the case screws back in and insert three AAA batteries into the battery compartment.

Your dialer is now ready to test. Switch the unit on. The LED on the dial pad side should be lit. Set the lower slide switch to STORE mode. Press the MEMORY button on the dial pad. Press the * key five times. Press the MEMORY key again and then press the P1 key. A beep tone should be heard when any key is pressed and a long beep should sound after the P1 key has been pressed to indicate that the programming sequence was performed correctly.

Switch the unit into DIAL mode. Press the P1 key, and five tone

pulses that sound remarkably like coin tones should come out of the speaker. I usually program P1 to be four quarters (insert one or two PAUSE's between each set of five tones), P2 to be two quarters, and P3 as one quarter.

Of course, you can no longer use the unit to generate touch tones.

History and Theory

A friend of mine and I were sitting around his house one day trying to come up with a way to build a reasonable red box. I had built one with analog sine wave generators in the past, but it was difficult to adjust the frequency of the outputs and keep them accurate over time and with changes in temperature. The electronic project box I had assembled it in was bulky, hard to conceal, and definitely suspicious-looking.

My friend was playing with his calculator while I was wishing that we had the money and time to design a microprocessor-controlled device with its own custom PC board. After a while, he announced that he had an idea. He had been looking at a data sheet for a DTMF (Dual Tone MultiFrequency aka touch tone) generator chip. He calculated the ratio of the coin tone frequencies of 1700 Hz and 2200 Hz to be 0.7727. He then went through all of the tone pairs used for DTMF, calculating each of their ratios. He discovered that the ratio of the tone pair used for * was very close to the ratio for the coin tone frequencies. This ratio, 941/1209=0.7783, differed from the coin tone ratio by less than one percent.

What this meant was that since the tones generated by such a chip are digitally synthesized from a divider chain off of a reference crystal, if one changed the reference crystal to the "right" frequency, the coin tones would be generated instead of the DTMF *. Most DTMF chips use a TV color-burst crystal with a frequency of 3.579545 MHz. To determine the crystal frequency that would generate the coin tones, one would compute 3,579,545 / 941 * 1700 = 6,466,766; 3,579,545 / 1209 * 2200 = 6,513,647; (6,466,766 + 6,513,647) / 2 = 6,490,206 MHz.

Unfortunately, this is not a standard crystal value and getting custom crystals made is a real pain for the hobbyist. The closest standard frequency I could find was 6.5536 MHz. I tried a crystal of this value and it worked.

(The actual frequencies produced by a DTMF generator chip depend on the particular manufacturer's design. The color-burst crystal's frequency is divided down to the DTMF tones by an integer divider chain. Because the color-burst crystal's frequency is not an integer multiple of the DTMF tones there will be a small difference in the frequencies produced from the standard.)

When we first tried this, we were using one of Radio Shack's earliest tone dialers. It consisted of a DTMF generator chip only, and as such could not produce a sequence of tones automatically. Tones were generated as long and as fast as

one could press the buttons. We were able to simulate nickels using this device but doing so was fairly slow and tedious. Because our manual timing was so far off of the mark, our attempts at producing dime or quarter signals were a miserable failure. A live operator would be instantly connected to the line whenever we tried it.

The Shack's next model had a microprocessor and a tone generator in it, each with separate crystals controlling their respective timing. It was just a matter of changing the micro's crystal to get the right on-off timing for a quarter's timing for a quarter's tone sequence as well as the tone generator's crystal to get the proper coin frequencies.

Later Radio Shack came out with the model used in this project. I promptly bought one because it was lower cost and more compact than their older model. I put some batteries in it and tried it out. It generated DTMF sequences with very long on and off times, but other than that, seemed like a nice unit. Upon disassembling it though, I became unhappy. There was only one crystal. It controlled the timing for a microprocessor that was specifically designed to synthesize DTMF. There was no way to independently adjust the output frequency of the tones from their on-off timing. I was just about to say, "Oh well, yet another tone dialer for my collection" when it hit me. Why not try the higher frequency crystal? The timing might come out close enough to simulate either a quarter or a dime. I made the mod and tested it out. It worked!

Thank you Radio Shack, for giving us a convenient to use, easily concealable and non-suspicious-looking red box.

Reference

The crystal is available from Fry's Electronics in Freemont, CA for $0.89 plus the charge for UPS Red or Blue. Their number is 415-770-3763. I would suggest buying five, some for future use and some just in case you cut the leads too short when trying this project.

Coin frequencies: 1700 Hz and 2200 Hz +- 1.5%.

Timing: 5 cents, one tone burst for 66 ms (milliseconds) +- 6 ms; 10 cents, two tone bursts each 66 ms, with a 66 ms silent period between tones; 25 cents, five tone bursts each 33 ms +- 3 ms with a 33 ms silent period between tones.

Nothing gives us more joy than seeing really interesting things show up on our fax machine. If you want to send us articles, clippings, letters, pictures, or anonymous information, why not fax us at (516) 751-2608? It's the nineties thing to do.

Howard Hughes
44 Westlyn Terrace
Montecito, CA 94945

June 14-90
19

5545

11-76/6774

Pay to the order of 2600 magazine $ 59,449.**

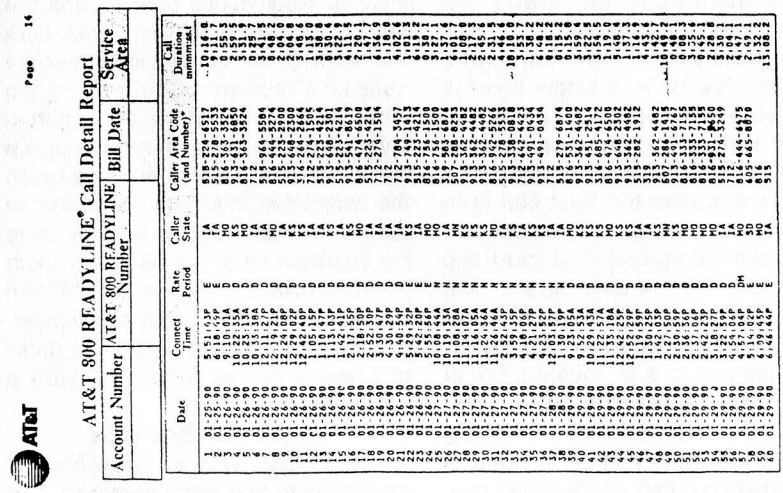
FiftyNine Thousand FourHundredFortyNine and **/100 DOLLARS

Bank of Montecito
P.O. Box 11
Montecito, CA 99496

MEMO E911 document

|: 23400028|:5545++29889

We want to thank everyone who took advantage of our Spring 1990 BellSouth E911 document offer. Now we really need you to help by contributing to the Neidorf Defense Fund. Details are on page 31.



AT&T 800 READYLINE® Call Detail Report

Page 14

Account Number	AT&T 800 READYLINE Number	Bill Date	Service Area

	Date	Connect Time	Rate Period	Caller State	Caller Area Code (and Number)*	Call Duration (mm:ss)
1	01-25-90	5:51:03P	E	IA	515-274-5517	10:16.0
2	01-25-90	8:11:19P	E	IA	515-274-5533	9:11.7
3	01-26-90	9:10:01A	D	MO	816-363-3824	0:55.5
4	01-26-90	10:22:35A	D	MO	816-358-5590	1:31.9
5	01-26-90	10:55:38A	D	MO	816-363-3924	0:43.7
6	01-26-90	10:55:38A	D	IA	712	0:48.5
7	01-26-90	12:11:21P	D	IA	712-944-5584	3:18.2
8	01-26-90	12:24:08P	D	MO	816-443-2274	2:04.0
9	01-26-90	12:24:08P	D	IA	515-225-2000	2:46.8
10	01-26-90	12:29:02P	D	KS	913-648-2464	2:46.8
11	01-26-90	1:05:15P	D	KS	913-648-2464	1:13.0
12	01-26-90	1:05:15P	D	IA	712-274-1505	1:13.0
13	01-26-90	11:10:47P	D	IA	515-223-3211	1:30.4
14	01-26-90	11:10:47P	D	IA	515-223-3211	1:30.4
15	01-26-90	1:42:41P	D	IA	515-225-4214	5:22.9
16	01-26-90	2:17:55P	D	KS	913-541-6619	4:11.1
17	01-26-90	2:52:30P	D	MO	816-842-5500	2:47.7
18	01-26-90	2:52:30P	D	IA	515-223-4214	2:47.7
19	01-26-90	3:30:47P	D	IA	712-274-1504	4:16.9
20	01-26-90	3:30:47P	D	IA	712	4:16.9
21	01-26-90	4:30:24P	D	IA	712-784-3457	4:02.6
22	01-26-90	4:30:24P	E	KS	913-749-1413	1:01.3
23	01-26-90	5:42:20P	E	KS	913-681-1504	6:38.2
24	01-26-90	5:42:20P	E	MO	816-761-1500	6:38.2
25	01-27-90	10:08:44A	N	MO	816-756-1500	5:27.1
26	01-27-90	10:19:35A	N	IA	507-265-8255	1:01.7
27	01-27-90	10:19:35A	N	IA	507-265-8255	1:01.7
28	01-27-90	11:14:07A	N	KS	913-362-4482	1:08.8
29	01-27-90	11:14:07A	N	KS	913-362-4482	2:55.5
30	01-27-90	11:16:05A	N	KS	913-362-4482	2:55.5
31	01-27-90	11:24:46A	N	MO	816-942-2666	2:31.5
32	01-27-90	2:52:45P	D	IA	515-278-0315	2:46.6
33	01-27-90	2:52:45P	D	IA	515-278-0315	10:33.7
34	01-27-90	4:18:06P	D	KS	913-491-0434	1:38.2
35	01-27-90	4:21:27P	D	KS	913-491-0434	1:38.2
36	01-28-90	12:03:37P	N	IA	712	0:18.2
37	01-28-90	1:30:19P	N	IA	712	0:15.2
38	01-28-90	1:30:19P	N	IA	515-270-1874	0:15.2
39	01-29-90	9:23:55A	D	MO	816-942-2666	3:59.4
40	01-29-90	9:23:55A	D	KS	913-362-4482	3:59.4
41	01-29-90	10:29:43A	D	KS	913-451-2114	3:22.5
42	01-29-90	11:22:37A	D	KS	913-451-2114	3:22.5
43	01-29-90	11:27:17A	D	MO	816-474-4500	1:19.0
44	01-29-90	12:42:25P	D	KS	913-648-2302	1:49.4
45	01-29-90	12:42:25P	D	KS	913-648-2302	1:49.4
46	01-29-90	12:52:29P	D	KS	913-362-1912	1:14.3
47	01-29-90	1:42:05P	D	KS	913-362-1912	1:14.3
48	01-29-90	1:50:59P	D	KS	913-491-2727	4:43.4
49	01-29-90	1:50:59P	D	KS	913-491-2727	0:48.1
50	01-29-90	2:16:36P	D	MO	816-333-7155	0:55.5
51	01-29-90	2:16:36P	D	MO	816-333-7155	0:55.5
52	01-29-90	2:42:23P	D	MO	816-333-7155	0:45.1
53	01-29-90	2:42:23P	D	MO	816-333-7155	0:45.1
54	01-29-90	3:18:27P	D	MO	816-931-9550	2:20.8
55	01-29-90	3:18:27P	D	MO	816-931-9550	2:20.8
56	01-29-90	4:55:06P	D	IA	712-546-4335	2:01.1
57	01-29-90	4:57:06P	E	MO	816-445-4335	2:01.1
58	01-29-90	4:57:06P	E	MO	816	2:01.1
59	01-29-90	4:09:45P	E	MO	816	13:32.2
60	01-29-90	6:46:44P	E	IA	515	13:08.2

* If available

Here we see what many 800 customers are now able to see: YOUR telephone number. There are still parts of the country that don't pass along ANI; they are shown as area codes only.

building a telephone

by 1000 Spiderwebs of Might

This multipurpose induction coil slips over the handset receiver of any payphone or standard desk phone and can be used in conjunction with a Walkman-type cassette unit for a variety of record and playback functions with excellent fidelity — at least to the extent that the telephone lines can carry frequency response-wise. You'll need a piece of brown corrugated cardboard from the side of a discarded box, some thin cardboard (like from a cereal box), a sharp hobby knife, electrician's tape, white glue or a hot glue gun (it'll speed construction a great deal) and 50 feet of #26 wire.

Begin by taping a single layer of cereal box type cardboard (about 1/2" wide) around the receiver side of the handset and secure it with a single wrap of tape. This is a spacer layer and is eventually discarded but insures the finished induction coil slides easily over the handset's receiver. Now wrap a single layer of 1/2" wide corrugated cardboard around this spacer layer and secure with a wrap of tape. Corrugated cardboard makes the best coil form because of its strength and rigidness.

Pull the corrugated cardboard ring off and discard the inner spacer ring (or save it if you are constructing more than one coil). Glue the corrugated cardboard ring to a 4" square piece of corrugated. After the glue sets, carefully cut out the inside of the ring with a sharp hobby knife to make a nice round hole that easily slides over the handset's receiver. Now glue another 4" square piece to the other side of the coil form and again cut out the inside of the ring.

Measure out about 50 feet of #26 wire and wind it around the completed corrugated coil core. Secure the two wire ends of the coil by twisting them together a few times. At this point you can either solder a short piece of shielded cable attached to an inline RCA phono jack or a longer cable terminated with a miniature stereo plug of the kind used in Walkman-type headphones. Connect the left and right channel inner conductors together for one connection to the coil and use the shielded braid for the other connection. If possible use a coil cord. They don't tangle as easily plus coil cords always have a cool hi-tech look to them.

Now carefully trim down the outside cardboard sides of the coil and wrap a long continuous overlapping spiral layer of electrician's tape around the remaining "doughnut" coil. Make sure the finished coil easily slides over the handset's receiver without being too loose or wobbly. Add another partial layer of tape if necessary to snug up the fit. For the ultimate finishing touch the completed induction coil could be dipped in "Plasti Dip" instead of using the insulated tape. It dries to a smooth uniform rubberized coating. "Plasti Dip" is usually used to dip screwdriver, wrench, or other tool handles in order to prevent corrosion and provide a better grip.

Make a Red Box Tape

The easiest way to make one by yourself is to find two payphones side by side (like at a shopping mall, airport, or hotel lobby). Plug in your induction coil to the tape recorder's

external mic input making sure you've installed fresh batteries. Pick up phone #1, slide on the induction coil (it's best to cover the mouthpiece with a thick cloth to block any extraneous sounds), start the recording mode and initiate a call to neighboring payphone #2. Answer it, press the mouthpiece against your chest to block out any noise and *slowly* deposit about $5 or $6 worth of quarters into payphone #2. Hang up phone #2 after the last coin and all your change will come back via the coin return after a few seconds delay. Now you have a red box tape of quarter tones ready to go.

Plug the induction coil into the earphone output jack of your tape recorder. Play back the series of tones — you'll hear them clearly reproduced through the earpiece. Adjust the volume control for a nice and clear reproduction. Usually the control will be a notch or two short of full volume. Now make a test long distance call to check out your new tape. Just don't let your batteries run down too low and you'll always get consistently good results. The tape can even be copied over to another Walkman-type recorder using an appropriate patch cord. It's best to record and play back the copied tape on the same cassette recorder because exact tape speed is important to keep the pitch of beep tones identical. If you want to play music or a prerecorded spoken message over the phone the induction coil will produce superior fidelity compared to the carbon mic element in the handset. While music fidelity isn't great over the rather limited frequency range of phone lines it's still OK — much better than you're used to hearing and at times it's fun to be able to do it conveniently. Since the induction coil couples all signals to the phone line via a magnetic field the fidelity is as good as possible and is only limited by the characteristics of the particular phone circuits.

(Turn page for pictures.)

STAFF

Editor-In-Chief
Emmanuel Goldstein

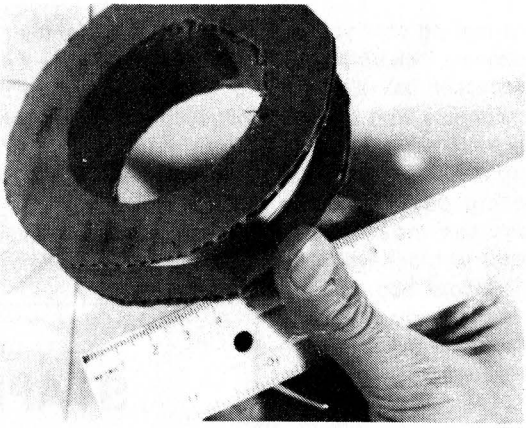
Artwork
Holly Kaufman Spruch

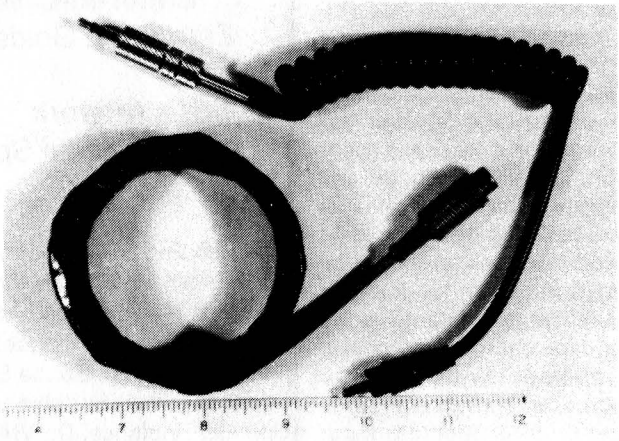
Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Log Lady, Craig Neidorf, The Plague, The Q, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Mr. Upsetter, Violence, Dr. Williams, and the unusual anonymous bunch.

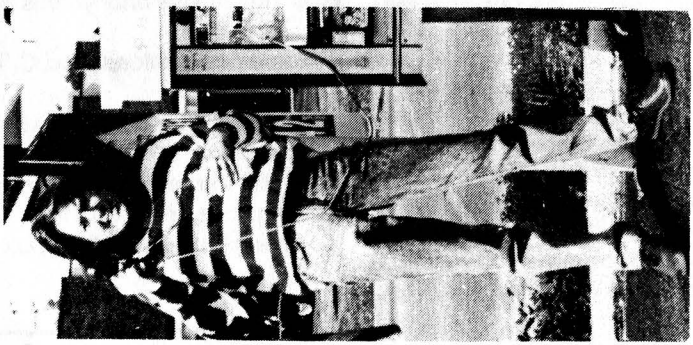
Remote Observations: Geo. C. Tilyou

Shout Outs: Steve for getting us through the last year, Franklin for the future, the electronic underground for refusing to die, and M.O.D. for continuing to allow us at their meetings.

the telephone induction coil







THE DEFINITIVE ANAC GUIDE

This is a numerical list of ANAC numbers for the United States. Dialing this number gives you your telephone number. If you don't see your area code here, try searching for your ANAC number and let us know when you find it. If you're having trouble using an ANAC listed below, try putting a 1 in front of it. If that doesn't work, the number may have changed or may not apply to your area.

205:::908-222-2222
212:::958
213:::114
213:::1223
213:::61056
214:::970-xxxx
215:::410-xxxx
217:::200-xxx-xxxx
217:::290
305:::200-222-2222
309:::200-xxx-xxxx
309:::290
312:::1-200-5863
312:::200-xxx-xxxx
312:::290
313:::200-222-2222
317:::310-222-2222
317:::743-1218
401:::222-2222
403:::908-222-2222
404:::940-xxx-xxxx
407:::200-222-2222
408:::300-xxx-xxxx
408:::760
409:::970-xxxx
414:::330-2234
415:::200-555-1212
415:::211-2111
415:::2222
415:::640
415:::760
415:::760-2878
415:::7600
415:::7600-2222
502:::997-555-1212
509:::560
512:::200-222-2222
512:::970-xxxx
516:::958
517:::200-222-2222
518:::997
518:::998
602:::593-0809
602:::593-6017
602:::593-7451
604:::1116
604:::116
604:::1211
604:::211
612:::511
615:::830
616:::200-222-2222
617:::200-xxx-xxxx
617:::220-2622
618:::200-xxx-xxxx
618:::290
713:::970-xxxx
714:::211-2121
716:::511
718:::958
806:::970-xxxx
812:::410-555-1212
815:::200-xxx-xxxx
815:::290
817:::211
817:::970-xxxx
906:::200-222-2222
914:::1-990-1111
914:::99
914:::990
914:::990-1111
915:::970-xxxx
919:::711

11953-0099

(continued from page 31)

jack (DFW). Others seem to be wide open and unrestricted to the world if you have a standard tone generator or can sing perfect pitch.

I have a PC with a modem but the only system I've been able to explore is the random interaction of a Wicom cordless telephone activated while I'm on line. The frequency sends garbage all over my screen and then the telco guys are under the street for weeks messing about with the local switches. I'm not sure if they are looking for a problem or add...g new monitors to my line. All very scary stuff.

A consideration for serious hackers may be an association similar to A.C.E. (Association of Clandestine Radio Enthusiasts). They had some sort of pool of funds to pay the FCC fines and legal fees for paid members who got caught. As the clampdown gets tighter we shall have to get more creative in our defenses.

Pirate cellular is growing fast. The programming sequence seems to be the key. I'm sure I'll have it soon. As dealers become busier, they are talking the owners through the setup procedure on the phone! Normally they are supposed to do it in the shop. I'll keep you posted.

First Phone, Integretel, and Midatlantic seem to all be using the same long distance lines these days. So when you get interrupted by an operator, they seem to have no idea whose customer you are. Access 950-1042 or 800-950-1042. Have a good go at them. They charge me 80 cents a minute to call my own call waiting!

Some other simple fun that I have had the pleasure of exploring is answering machines. An article on this subject would be easy to compose. All of the remote access codes are printed inside the cover or on a sticker on the bottom of the machine at your local department store, answering machine section. Playback and room monitor seem very harmless, while reset, OGM record, and on/off could cause you some trouble. Most of these can be hit with a general scan of the tones. An innovative application was played by teenagers calling on my business 800 lines over the weekend from different payphones and leaving messages for their friends to retrieve from any other payphone in the country. The cheapest way to stop them was to put in a very old machine without tone remote.

NB
Rhode Island

2600 BACK ISSUES

What a great gift idea for the holidays! (Beats the hell out of *Sports Illustrated*)

2600 has covered a lot of ground since 1984. If you haven't been with us for the entire journey, we think you'll find this bit of history enlightening, educational, and entertaining (the 3 e's). Our back issues are sold by the year ($25/$30 overseas, US funds only). Use the order form on Page 47 and mail it to:

2600 Back Issues
PO Box 752
Middle Island, NY 11953
Allow 4-6 weeks for delivery.

2600 Marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011,212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

WANTED: Red and blue box plans/kits and assembled kits. Also, expansion cards for a 256K Compaq. Please contact Charles Silliman, 11819 Fawnview, Houston, TX 77070.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

WANTED: Atari ST hacking/telecom programs to trade. I have Mickey Dialer and 2 tone generation programs. Nil, PO Box 7516, Berkeley, CA 94707.

WANTED: Hacking and phreaking software for IBM and Hayes compatible modems. Wardialers, extender scanners, and hacking programs. Advise cost. R.T., PO Box 332, Winfield, IL 60190.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

NEW FROM CONSUMERTRONICS: "Voice Mail Hacking" ($29), "Credit Card Scams II" ($29), Credit Card Number Generation Software (inquire). More! Many of our favorites updated. New Technology Catalog $2 (100 products). Need information contributions on all forms of technological hacking: 2011 Crescent, Alamogordo, NM 88310. (505) 434-0234.

RARE TEL BACK ISSUE SET. (Like TAP but strictly telephones.) Complete 7 issue 114 page set $15 ppd. TAP back issue set-320 pages-full size copies NOT photo-reduced $40 ppd. Pete Haas, P.O. Box 702, Kent, Ohio 44240.

VIRUSES, TROJANS, LOGIC BOMBS, WORMS, and any other nasties are wanted for educational purposes. Will take an infected disk and/or the source code. If I have to, I will pay for them. Please post to: P. Griffith, 25 Amaranth Crt, Toronto, ONT M6A 2P1, Canada.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

WANTED: Audio recordings of telephone related material. Can range from recordings of the past and present to funny phone calls to phone phreaking. Inquire at 2600, PO Box 99, Middle Island, NY 11953. (516) 751-2600.

VMS HACKERS: For sale: a complete set of DEC VAX/VMS manuals in good condition. Most are for VMS revision 4.2; some for 4.4. Excellent for "exploring"; includes System Manager's Reference, Guide To VAX/VMS System Security, and more. Mail requests to Roger Wallington, P.O. Box 446, Leonia, NJ 07605-0446.

Deadline for Winter Marketplace: 1/1/91.

AN ALGORITHM FOR

by Crazed Luddite & Murdering Thug
K00l/RaD Alliance!

As some of you know, the credit card companies (Visa, MC, and American Express) issue card numbers which conform to a type of checksum algorithm. Every card number will conform to this checksum, but this is not to say that every card number that passes this checksum is valid and can be used, it only means that such a card number can be issued by the credit card company.

Often this checksum test is used by companies which take credit cards for billing. It is often the first step in checking card validity before attempting to bill the card, however some companies stop here. Some companies only check the first digit and the card number length, others use this very convenient algorithm, while others continue on to check the bank ID portion of the card number with a database to see if it is a valid bank. These tests are designed to weed out customers who simply conjure up a card number. If one were to try and guess at an Amex number by using the right format (starts with 3 and 15 digits long), only about 1 in 100 guesses would pass the checksum algorithm.

Why do companies use the algorithm for verification instead of doing an actual credit check? First, it's much quicker (when done by computer). Second, it doesn't cost anything. Some credit card companies and banks charge merchants each time they wish to bill or verify a card number, and if a merchant is in a business where a lot of phony numbers are given foı verification, this can become rather costly. It is a known fact that most, if not all, online services (i.e. Compuserve, Genie, etc.) use this method when processing new sign-ups. Enough said about this, you take it from there.

The majority of transactions between credit card companies and merchants take place on a monthly, weekly, or bi-weekly basis. Such bulk transactions are much less expensive to the merchants. Often a company will take the card number from a customer, run it through the algorithm for verification, and bill the card at the end of the month. This can be used to your advantage, depending on the situation.

If you trade card numbers with your friends, this is a quick way to verify the numbers without having to call up the credit card company and thus leave a trail. Also, a few 1-800 party line type services use this algorithm exclusively because they don't have a direct link to credit card company computers and need to verify numbers real fast. Since they already have the number you're calling from through ANI, they don't feel it necessary to do a complete credit check. I wonder if they ever heard of pay phones.

Here's how the algorithm works. After the format is checked (correct first digit and correct number of digits), a 21212121... weighing scheme is used to check the whole card number. Here's the english pseudocode:

```
check equals 0.
go from first digit to last digit
 product equals value of current digit.
 if digit position from end is odd
  then multiply product by 2.
 if product is 10 or greater
  then subtract 9 from product.
 add product to check.
end loop.
if check is divisible by 10, then card passed
checksum test.
```

Here is a program written in C to perform the checksum on a Visa, AMEX or MC card. This program can be easily implemented in any language, including ACPL, BASIC, COBOL, FORTRAN, PASCAL or PL/I. This program may be modified, with the addition of a simple loop, to generate credit card numbers that pass the algorithm within certain bank prefixes (i.e. Citibank). If you know the right prefixes, you can actually generate valid card numbers (90 percent of the time).

CREDIT CARDS

```
/* CC Checksum Verification Program
  by Crazed Luddite and Murdering Thug
 of the K00l/RaD Alliance! (New York, London, Paris, Prague.)
  Permission is granted for free distribution.
  "Choose the lesser of two evils.  Vote for Satan in '92"
*/

#include <stdio.h>
main()
{
 char cc[20];
 int check, len, prod, j;
 printf("\nAmex/MC/Visa Checksum Verification Program");
 printf("\nby Crazed Luddite & Murdering Thug\n");
 for (;;)
 {
 printf("\nEnter Card Number [w/o spaces or dashes.] (Q to quit)\n:");
 scanf("%s",cc);
 if ((cc[0]=='Q')||(cc[0]=='q')) break;  /* exit infinite loop, if 'Q' */

 /* Verify Card Type */

 if ((cc[0]!='3')&&(cc[0]!='4')&&(cc[0]!='5'))
   {
    printf("\nCard number must begin with a 3, 4, or 5.");
    continue;
   }
 else if ((cc[0]=='5')&&(strlen(cc)!=16))
   { printf("\nMasterCard must be 16 digits.");
    continue;
   }
 else if ((cc[0]=='4')&&(strlen(cc)!=13)&&(strlen(cc)!=16))
   { printf("\nVisa numbers must be 13 or 16 digits.");
    continue;
   }
 else if ((cc[0]=='3')&&(strlen(cc)!=15))
   { printf("\nAmerican Express numbers must be 15 digits.");
    continue;
   }

 /* Perform Checksum - Weighing list 2121212121212121.... */

 check = 0;                  /* reset check to 0 */
 len = strlen(cc);
 for (j=1;j<=len;j++)        /* go through entire cc num string */
 {
  prod = cc[j-1]-'0';        /* convert char to int */
  if ((len-j)%2) prod=prod*2;    /* if odd digit from end, prod=prod*2 */
                 /* otherwise prod = prod*1 */
  if (prod>=10) prod=prod-9;     /* subtract 9 if prod is >=10 */
  check=check+prod;          /* add to check */
 }
 if ((check%10)==0)          /* card good if check divisible by 10 */
  printf("\nCard passed checksum test.");
 else
  printf("\nCard did not pass checksum test.");
 }
}
```

FACTS AND

Over the past year there has been a great deal of publicity concerning the actions of computer hackers. Since we began publishing in 1984 we've pointed out cases of hackers being unfairly prosecuted and victimized. We wish we could say things were getting better but we cannot. Events of recent months have made it painfully clear that the authorities, above all else, want to "send a message". That message of course being that hacking is not good. And there seems to be no limit as to how far they will go to send that message.

And so we come to the latest chapter in this saga: the sentencing of three hackers in Atlanta, Georgia on November 16. The three, Robert Riggs (The Prophet), Frank Darden, Jr. (The Leftist), and Adam Grant (The Urville) were members of the Legion of Doom, one of the country's leading hacker "groups". Members of LOD were spread all over the world but there was no real organization, just a desire to learn and share information. Hardly a gang of terrorists, as the authorities set out to prove.

The three Atlanta hackers had pleaded guilty to various charges of hacking, particularly concerning SBDN (the Southern Bell Data Network, operated by BellSouth). Supposedly Riggs had accessed SBDN and sent the now famous 911 document to Craig Neidorf for publication in PHRACK. Earlier this year, BellSouth valued the document at nearly $80,000. However, during Neidorf's trial, it was revealed that the document was really worth $13. That was enough to convince the government to drop the case.

But Riggs, Darden, and Grant had already pleaded guilty to accessing BellSouth's computer. Even though the facts in the Neidorf case showed the world how absurd BellSouth's accusations were, the "Atlanta Three" were sentenced as if every word had been true. Which explains why each of them received substantial prison time, 21 months for Riggs, 14 months for the others. We're told they could have gotten even more.

This kind of a sentence sends a message all right. The message is that the legal system has no idea how to handle computer hacking. Here we have a case where some curious people logged into a phone company's computer system. No cases of damage to the system were ever attributed to them. They shared information which we now know was practically worthless. And they never profited in any way, except to gain knowledge. Yet they are being treated as if they were guilty of rape or manslaughter. Why is this?

In addition to going to prison, the three must pay $233,000 in restitution. Again, it's a complete mystery as to how this staggering figure was arrived at. BellSouth claimed that approximate figure in "stolen logins/passwords" which we have a great deal of trouble understanding. Nobody can tell us exactly what that means. And there's more. BellSouth claims to have spent $1.5 million tracking down these individuals. That's right, one and a half million dollars for the phone company to trace three people! And then they had to go and spend $3 million in additional security. Perhaps if they had sprung for security in the first place, this would never have happened. But, of course, then they would have never gotten to send the message to all the hackers and potential hackers out there.

We think it's time concerned people sent a message of their own. Three young people are going to prison because a large company left its doors wide open and doesn't want to take any responsibility. That in itself is a criminal act.

We've always believed that if people cause damage or create a nuisance, they should pay the price. In fact, the LOD believed this too. So do most hackers. And so does the legal system. By blowing things way out of proportion because computers were involved, the government is telling us they really don't know what's going on or how to handle it. And that is a scary situation.

If the media had been on top of this story and had been able to grasp its meaning, things might have been very different indeed. And if BellSouth's gross exaggerations had been taken into account at the sentencing, this injustice couldn't have occurred. Consider this: if Riggs' sentence were as much of an exaggeration as BellSouth's stated value of their $13 document, he would be able to serve it in full in just over two hours. And the $233,000 in restitution would be under $40. So how much damage are we really talking about? Don't look to BellSouth for answers.

In early 1991, the three are to begin their

sentences. Before that happens, we need to reach as many people as possible with this message. We don't know if it will make a difference in this particular case if the general public, government officials, and the media hear this side of the story. But we do know it would be criminal not to try.

***

When we needed to get the word out on the Neidorf story, we learned something about the power of electronic communications. By making use of the Internet, the story spread throughout the globe rapidly and responses poured back. One computer system in particular, The Well, located in the Bay Area of California and affiliated with The Whole Earth Review was an instrumental tool in opening those communications. We hope to see many other affordable multi-user systems that offer lively discussions and useful services in the future. We encourage our readers to get involved in this technology before participation in it becomes regulated and restricted by those who don't appreciate it. You can register online at The Well by calling 415-332-6106.

***

In another tale of nobody really knowing what's going on, two teenage brothers were arrested in November and charged with causing $2.4 million worth of damage to a voice mail system. It seems that the kids were promised a poster with their subscription to Games Pro Magazine. When they didn't get it after repeated complaints, they figured out how to get into the company's voice mail system. They were able to get into 200 different mailboxes, including that of the company president. The company accuses the brothers of wiping out messages, changing passwords, and changing user names. A company official expressed surprise that they were able to change names, claiming that it was not an easy thing to do.

If, as has been reported, the voice mail system was Rolm's Phonemail, the company is almost totally responsible for what happened to them. Phonemail allows passwords to be up to 24 digits in length. These clowns apparently left their passwords as the default, which is usually a mere three digits. Hence the ease of entry. And the fact that the system administrator left his/her password as the default explains how they were able to change user names so easily. A child could do it.

Not many people will claim that what these kids did was acceptable. But the way the authorities handled this was absurd, at best. Kids have always done mischievous things and they always will. And no matter how hard the authorities try, they're not going to find any conspiracy here. These were kids being naughty and taking advantage of incompetence. A stern warning would undoubtedly have put an end to it. Instead, they're being charged with all kinds of federal crimes and told that they caused $2.4 million in damage. And the U.S. Secret Service and the New York State Police seem real proud of this.

***

Speaking of the New York State Police, according to a report from the news service Newsbytes, Donald Delaney, New York State Police Special Investigator, admits to spying on 2600 meetings at the Citicorp Center in New York City. Spies working for him took pictures of people as they attended the monthly gatherings. It seems pretty absurd that they would waste their time sneaking around when we're having a public meeting right smack in the middle of midtown Manhattan. Add to this the fact that we discovered them doing this back in the spring (see Spring 1990 issue) and one gets the distinct impression that these folks haven't yet found their niche in society.

***

In a typical case of jumping on the bandwagon, a New York therapist is attempting to get some new clients out of a recent hacker story. "According to Jonathan Berent," his press release reads, "director of Berent Associates Social Therapy Center in Great Neck, NY, [the story of ZOD, a recently raided hacker] illustrates classic symptoms of social phobia — defined as the extreme fear and avoidance of people outside of one's immediate family. Mr. Berent explains that 'social phobics often turn to computers in an attempt to create a substitute for the social interaction with friends that they find lacking in their daily lives. Additionally, they frequently exhibit denial — they deny that any social problem exists. They claim that they have plenty of friends — but just choose to spend their free

FACTS AND RUMORS

time with the computer instead of peers. Other characteristics of social phobia include fear of people, anxiety attacks in social situations, overdependence upon parents, difficulty with social skills, and family chaos. Another key characteristic of social phobia is anger coupled with destructive behavior. This may explain the $250,000 worth of [completely unsubstantiated as usual] computer system damages that ZOD has been accused of.'

"According to Mr. Berent, social phobia often leads to addictive behaviors — including addictions to computers, telephone party lines, television — even addiction to avoidance itself. Far from a mere passing phase, Jonathan Berent explains, 'Social phobia has a tendency to get worse and worse if left alone. Fortunately, however, it has been proven that social phobia is a controllable and curable problem. In our program of individual and social group therapy, we have seen countless recoveries from social phobia through clients' learning first to control their anxiety, and then learning the specific social skills that underly social success. Through goal-oriented therapy and programs that offer an opportunity for social practice, we have been able to help facilitate social phobics in breaking through their self-imposed limitations to form quality relationships — often for the first time in their lives — and live much happier lives as a result.'

"Mr. Berent has been working with social phobics for over 10 years."

Imagine that. A cure for hacking. Will wonders never cease?

***

Last issue we printed a number that read back whatever phone number you were calling from, nationwide. Our readers found this useful for payphones, tie-lines, airplane phones, or any situation where knowing the telephone number they were using was important or just interesting. Unfortunately that number has stopped working. But a new number has surfaced: 800-933-3258....Wisconsin Bell is the latest of the phone companies to drop the charge for touch tone service. We won't rest until they've all been eliminated. Speaking of rate changes, New York Telephone asked the state Public Service Commission for an $831.7 million (13 percent) rate increase earlier this year. Many people were outraged by this request. So, apparently, were the PSC administrative law judges, who recommended a rate increase of only $23.6 million (0.37 percent). In fact, after reports surfaced of wild NYNEX sex parties as well as other unethical business practices, the PSC decided to explore the possibility of forcing New York Telephone to divest itself from NYNEX. Not all public servants keep their heads in the sand, something these companies ought to keep in mind....With regards to rip-offs: did you know it costs less to call an international sex line than it does to call a local one? That's right, we saw advertisements for sex lines in the Netherlands Antilles (011-599-2424, 2626, and 6262) right next to all of those other ads. The ironic thing is that most people see the 011 and figure the call will cost more. Guess again....Both Sprint and AT&T are offering free fax services related to the Gulf Crisis. By calling Sprint at 800-676-2255 you can direct a fax update to any fax machine in the country. And AT&T is offering Desert Fax. By going to an AT&T Phone Center and filling out an official fax form, you can have that fax sent to anyone in active duty in the Gulf. They won't tell us how exactly they do it. Sorry....AT&T is accusing MCI of stealing 90,000 customers over the last six months. Nothing new there, but according to Reuters, there's now a name for this practice. Changing a customer's long distance service to another company without permission is called "slamming". Would we lie?....Finally, a light-hearted story: in early November, police in Montgomery County, Alabama were testing the new E911 system. The dispatcher received ten consecutive calls from the home of Linda and Danny Hurst. When the police arrived at the Hurst house, the culprit was soon found: an overripe tomato. The tomato was hanging over the telephone in a wire basket, dripping juice into the couple's answering machine. Apparently the juice got into the machine's dialing system and caused it to dial the police. "We're not sure how," Chief Deputy Milton Graham said. "Maybe they had speed dialing and it shorted out." Linda Hurst also was baffled. "I didn't know the answering machine could even dial out. It's just supposed to take messages."

DON'T MAKE THAT MISTAKE

Many people do. They intend to renew, but the drudgeries of daily life get in the way. And then, one day, they realize that there's something missing. You see, we don't pester you repeatedly like most other magazines when your subscription runs out. You won't get phone calls, postcards, telegrams, faxes, or knocks on your door. We accept rejection gracefully. The tragedy occurs when subscribers **forget** to renew. Go look at your address label now. If you've only got an issue or two left, renewing today makes a whole lot of sense. And by renewing for multiple years, you'll have one less thing to worry about in a decade that promises to have plenty of worries.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988,1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED: _____

within...

caller i.d.	4
network 2000 saga (cont.)	8
dorothy denning interview	10
things you shouldn't know	16
defeating trap tracing	22
letters	24
tone dialer conversion	32
build a telephone induction coil	36
the definitive anac guide	39
2600 marketplace	41
credit card algorithm	42
facts and rumors	44

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733
ISSN 0749-3851

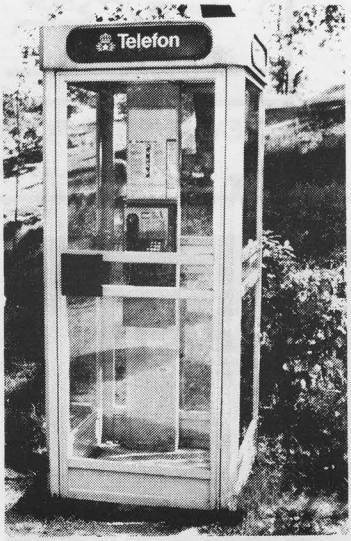
the threat
is real

2600

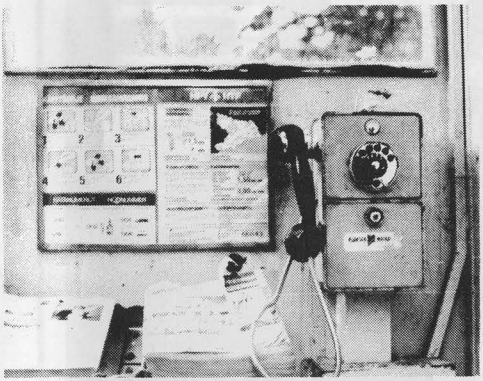
The Hacker Quarterly

VOLUME SEVEN, NUMBER FOUR
WINTER, 1990

SCANDINAVIAN PAYPHONES



A SWEDISH PAYPHONE AT DJVRGARDSBRON, STOCKHOLM



FINNISH PAYPHONE ON THE ISLAND FORTRESS OF SUOMENLINNA (SVEABORG), HELSINKI

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. SPECIAL PRIZE FOR AFRICAN PAYPHONES.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1990, 1991 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada --$18 individual, $45 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESS: 2600@well.sf.ca.us.

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein / Alan Smithee

Artwork
Holly Kaufman Spruch

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Log Lady, Craig Neidorf, The Plague, The Q, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Mr. Upsetter, Violence, Dr. Williams, and the anonymous many.

Remote Observations: Geo. C. Tilyou

Shout Outs: The subterranean chapter: Find the Power; dd: your Day will come, we promise; SS: thanks for making it interesting; Franklin; the few who have the strength to face the many; Screaming Target and the future; the millions held hostage.

a political

According to the *Philadelphia Inquirer,* a Republican staff member gained access to as many as 1,000 computer files and documents belonging to Democrats. The GOP staffer, Jeffrey Land, is reported to have admitted tapping into their files "many, many times" between July 1988 and the spring of 1990. Land was apparently able to gain access to files detailing "campaign contributions and the 1991 campaign strategy of the New Jersey Senate Democrats.

What's particularly appalling is that a secret legislative report indicates that his activities were known by his superiors who saw nothing wrong with what he was doing. "No one thought it appropriate to bring this fact to anyone's attention or deemed this to constitute an ethical breach," the report said.

A letter recently received by *2600* claims to reveal some inside information on this case. We'll let you be the judges.

I'd rather not divulge my real name, nor can I divulge my employers' names, not in light of an ongoing criminal investigation. Suffice it to say that I work for one of the two major political parties within the State of New Jersey and that, for the time being, I wish to maintain this job for a little while longer.

I report to the party leadership. I have been involved in politics for quite some time and now do a wide range of duties, among them issues of telecommunications security.

My telecommunications security skills, though hardly noteworthy in the presence of *2600's* readership, are somewhat respectable and tremendously aided by publications such as yours. This is why I wish to return a favor and contribute some of my insight for everybody's benefit.

Up front, I have been privy to much of what is going on in regards to the Jeffrey Land case.

Mr. Land was a former Assembly Aide to an Assemblyman, an assemblyman who, coincidentally, was among those implicated in the Pete Rose scandal (this assemblyman wrote a letter of recommendation on behalf of the guy who was indicted for participating in a cocaine ring selling to Rose).

"The Legislative Network is one system divided into sub-systems. It isn't too hard to get into one sub-system and out the other."

Land was smart. We were considered to be among the "bright boys".

Back in '88, we inadvertently broke through the user system of the WANG Legislative Network Systems and had found ourselves within the Systems Administrators' controls.

hacking scandal

I didn't stick around for too long. The only information I gained was a better understanding of how the system worked, but not the contents of the individual files stored within.

Land also busted through the users' system but didn't back out. He kept going on his own, all through '88, '89, and up to February of 1990 when he finally got caught.

The Land case is fascinating. It's been in the news around here for some time. Land had not only gotten into the system, but had also taken out interesting information, like contributor listings, campaign strategies, and such — all from the opposing political party.

The Legislative Network, you see, is one system divided into sub-systems. It isn't too hard to get into one sub-system and out the other. This is essentially what Land did.

Inquiries by the State Ethics Committee determined that the party leadership whom Land was working for was not only aware of this, but "saw nothing wrong in what he was doing."

Incredible. What's even more fascinating is that the opposing political party whose files have been exposed are not seeking to press any charges and wish to instead "forget about the whole thing." This, despite the acknowledged fact that Land managed to see and/or obtained well over 1,000 individually protected files!

Why back down?

Here's why.

Land uncovered solid, hard evidence including:

1) State staff, hired solely for the benefit of service to the public were working solely for the benefit of the elected officials on public money and time using public facilities, notably computer databasing facilities and the like. Public tax money for state staff salaries was therefore used to keep elected officials in office. Everybody does this, *but it's not supposed to be known outside of the office.*

2) Land's computer evidence directly correlates between given contributions and posted legislation. The major stumbling block for election-law overseers is that you cannot readily tell who is being given what. PAC (Political Action Committee) money is handed out in such a way that election law reports do not readily tell who actually benefits from these contributions. PAC's are deliberate fronts for corporations and others who do not want to leave a trail. Land obtained evidence showing what corporation gained what piece of legislation — tax breaks, funding loopholes, etc. — in a manner never done before.

"How can we reasonably expect our legislators to legislate on our behalf on such crucial telecommunications matters when they are, in fact, among those breaking the law?"

More Weirdness

Election-law controls are obviously

a hacking

in need of expansion. In light of what happened in the fall of '89, the Land case underlines this point. During October of '89, the current majority leadership members were implicated in a so-called "shake-down" of a lawyer's PAC. Among the so-called statements said to the lawyer's PAC representatives during that fateful dinner meeting was the now famous line: "Your members are going to be upset if your bills don't get posted." The FBI and the Attorney General's office later exonerated them of the allegations, but a bad taste still lingers.

We've all known about this shit; corruption is as old as the human race. A politician taking money — so what else is new? The catch is how can we reasonably expect our legislators to legislate on our behalf on such crucial telecommunications matters when they are, in fact, among those breaking the law? *Our legislators are among those encouraging partisan hacking!*

"It's not how you play the game, it's whether you win. Winning is, after all, everything."

I recall vividly what our director for our legislative staff said to me: "It's not how you play the game, it's whether you win. Winning is, after all, everything."

Great.

It is utterly ironic that, when approached upon the issue of "hackers" and the like, legislators crank out their "total distaste toward these individuals" while all along whatever information hackers cull they greedily accept, seeing "no apparent ethical wrongdoing" as Land's superiors so stated.

The State Attorney General's office announced that they "see no need to further investigate the matter." The Speaker of the House said that "the public doesn't give a tinker's damn about the situation." The argument flowing to the newspapers about the "fundamental separation of powers between the legislative and the executive branch of government" is garbage. The separation argument is, actually, a means of ducking the real issue: election funding reform. Ironically, both partisan political parties, Republican and Democrat, do agree upon avoiding this one issue as next year's elections are looming on the horizon.

I write this because you state in your article on "Operation Sundevil" that we should write to our legislators. Actually, as one who works closely with legislators, they really don't "give a tinker's damn", unless, of course, you're a large, multi-national PAC. After helping to set up the fundraisers, I've watched the legislative bills get posted and know *there's no such thing as coincidence at the state capital.*

I, for my part, feel that this country is rapidly becoming a tremendously twisted nightmare; it's one thing to have soldiers goosestepping down

political scandal

Pennsylvania Avenue, but something else when we're living within a giant David Lynch sitcom.

It is time that we start politicizing ourselves. (*Ha!* A hacker's PAC, anyone?!) It's time to start working together before more shit comes down the pike. Expect to see regulations, BBS licensing, and the like to come about, all in the name of raising taxes for these "tough economic times". Taxation and operational regulations are what the Secret Service and the legislators want, both as a means of a "better regulatory/law enforcement" and for raising more money to channel into other programs or job perks for relatives on the payrolls.

"The computer expert is becoming the samurai of these petty lords."

Never mind, though, that most of the boards would go under due to lack of sufficient funds to keep them going. This scenario also doesn't mention that those remaining BBS's would do so only by charging or increasing their operational charges. Our cutting edge gets dull and us with it — unless, of course, you've become a member of The New Movement, the Underground Net.

It's Getting Cold Around Here

Several other trends are becoming evident: the winnowing of Freedom of Information Act file acquisitions (see June of '90 American Bar Association Magazine), the lack of accountability on the part of credit bureaus obtaining private information from branches of the U.S. government (isn't it an amazing coincidence that TRW, the credit bureau, is also TRW, the major defense industry corporation?), and now the crackdown on BBS's — yep, surf's up: the stormtide's rising, gang.

The Lords of Disorder

Watergate lives on. I was recently hired by a congressperson on their campaign telecommunications/-databasing system. Somebody broke into this congressperson's system and got a listing of the major databases. No disks were stolen or damaged, not that anything ever is, and the office doors were, interestingly enough, not forced open. After an "inter-office investigation", custodial staff was found to have been "lax" and, although not proven, it appears that it was a primary election candidate's worker who managed to get in and check out the files.

This was bad. Once you know when, where, who, and what voting block your opponent is gunning, well, then you're fucked. Political strategy must then be shifted accordingly, and this can be a real pain in the ass.

This last story and the Land case illustrates how the computer expert is becoming the samurai of these petty lords, particularly those experts who stand on "the edge". Perhaps herein lies our true strength.

We are far stronger than what we're given to be; this is why the SS is strong-arming us and why corrupt politicians employ our skills while yet taxing our life's blood.

THE HACKER

by Dr. Williams

This article lists sources of computer security information of interest to hackers. The list is divided into six parts: underground magazines, catalogs, books, journals, newsletters, and network mailing lists. Each is given a brief description and information is provided on obtaining the product. This list is not intended to be comprehensive.

The information presented on the profiled magazines is up to date for the most part; a few sources are up to 18 months old. Therefore, before sending money, confirm the address and subscription rate by contacting the company. Some companies will send sample issues if asked.

Subscription rates denoted by "*freebie" indicates the magazine is free to qualified people. To become a qualified person, contact the company and tell them of your desire to receive their magazine. They will send a confirmation card asking some questions, including your company and job title. Good occupational choices are System Consultant or System Administrator.

Underground Magazines

TAP. After several revival attempts by various groups after the original, one of them managed to succeed. Written with the same flavor as the old *TAP,* but does not pick up where the old *TAP* left off. The anarchist-technical voice is there, but the chaotic shoe-string budget effect and loud voice is missing. Published whenever they have material to create an issue. Subscription rates are $10 a year, ($15 for Canada, $20 for overseas). Address: TAP, P.O. Box 20264, Louisville, KY, 40250.

Processed World. The magazine with the bad attitude towards technology. An analytically oriented, office centered magazine about work. Specifically its concerns are the drawback of work in a technological society with their "Tales of Toil" from around the area. $12 for 4 issues. Address: 41 Sutter St. #1829, San Francisco, CA 94104.

Fractal Report. A newsletter for those reasonably skilled in programming who wish to explore computer images of the Madelbrot set and its relatives. It's a shame they don't have color printing, but even the monochrome screen dumps here are rather interesting. Languages used include C, Pascal, and Forth. $23 for six issues. Address: J. de Rivax, c/o Fractal Reeves Telecommunications, West Town House, Porthtowan, Cornwall, TR4 8AX, United Kingdom.

The Capital District Computer Mart. A local magazine available by mail. In addition to the ads from area computer stores, they've got reviews and feature articles. Information useful to everyone is in every issue. $2 for four issues. Address: P.O. Box 402, Schenectady, NY 12301.

The Amateur Computerist. This forum grew out of a programming class for workers at Ford. It's sort of an experiment in bringing computing ideas to the shop floor grassroots. Mostly it's history and short programs in basic. Hasn't really taken off yet, but the potential is there. $5 for four issues. Address: R. Hauben, P.O. Box 4344, Dearborn, MI 48126.

Puget Sound Computer User. A local newspaper from the Seattle area with widespread appeal. Most articles cover topics of concern to everyone. Only the ads and events are local. $12 a year. Address: Puget Sound Computer User, 3530 Bagely Ave. N., Seattle, WA 98103, phone 206-547-4950.

Full Disclosure. A magazine for citizens interested in knowing and exercising their rights to the maximum legal extent. Emphasis placed on knowing rights against legally empowered authorities. $24 for twelve issues, published irregularly. Address: Full Disclosure, P.O. Box 8275, Ann Arbor, Michigan, 48107.

Cybertek. A better than usual survival/technological magazine. Computer anti-security mixed in with surveillance and survival. $15 for a year, $20 overseas. Published six times a year. Address: Cybertek Magazine, P.O. Box 64, Brewster, NY 10509.

Intertek. "The Cyberpunk Journal". A new publication on high tech. Single issues are $2.50, a year's subscription is $7. Address: Intertek, 325 Ellwood Beach, #3, Goleta, CA 93117. Make checks out to Steve Steinberg.

Hack-Tic. Holland's answer to 2600. $24 by international money order. Address: Hack-Tic, P.O. Box 22953, 1100 DL, Amsterdam, The Netherlands.

Catalogs of Books

Loompanics Unlimited. Self proclaimed publishers and sellers of unusual books, and they're right. Their catalog deals with most every subject. Areas the books are classified by: the underground economy, making money, tax evasion, privacy and hiding things, fake ID, big brother is watching, conducting investigations, crime and police science, frauds and con games, computer crime, locks and locksmithing, ninja, self defense, revenge, guns, silencers, knives, bombs and explosives, guerrilla warfare, murder and torture, survival, head for the hills, self sufficiency, gimme shelter, health and life extension, paralegal skills, sex, drugs, and rock and roll, intelligence increase, science and technology, heresy/weird ideas, anarchism and egoism, reality creation, and self-publishing. $2.50 for a catalog of books. Address: Loompanics Unlimited, P.O. Box 1197, Port Townsend, WA 98368.

Consumertronics. Like the Loompanics catalog, except more focused on technology and more aggressive, if that's possible. Sometimes they're successful, sometimes not. Information published in newsletter format, not books. As a result, less information is covered, but what is there is hard-

READING LIST

packed; a "how to" style is presented. Areas covered: computers, energy theft, phones, rip-offs, survival, and other technology and governmental agencies issues. $1.00 for a catalog. Address: Consumertronics, 2011 Crescent Dr., P.O. Box Drawer 537, Alamogordo, NM 88310.

CRB Research Books, Inc. Biggest selection of books describing all sorts of wireless communication: scanning frequencies, eavesdropping, jamming, CB's, shortwaves, radio directories, etc., plus the usual assortment of books dealing with underground technology, with a mishmash of other interesting books. $1.00 for a catalog. Address: CRB Research Books, Inc., P.O. Box 56, Commack, New York 11725.

FactSheet Five. The best, and only, complete source of underground magazines currently published — magazines which have anywhere from one to thousands of subscribers. Lists and reviews most current underground magazines in a catalog-type format. Contains a good number of magazines that are published outside the United States as well. Editor Mike Gunderloy does an excellent job describing and evaluating each "fanzine" in a paragraph. His reviews are objective, pointing out both good and bad features. These objective reviews are accurate most every time.

Most of the underground fanzines available can be plugged into one of these categories: political, poetry, musical, sports, anarchy, science fiction, entertainment, philosophy, religious, comics, current topics, sub-culture, sex, special interest, and various rantings and ramblings. *Factsheet Five* reviews pamphlets, books, and audio as well. $3.00 per issue. Address: Mike Gunderloy, 6 Arizona Avenue, Rensselaer NY 12144-4502. 24-hour answering machine (518) 479-3707. 300/1200/2400 baud computer bulletin board (518) 479-3879.

Catalogs of Products

Advanced Electronic Technologies. Product categories available: non-lethal weapons, transmitter detectors, telephone recorders, telephone tap detectors, parabolic microphones, microwave detectors, "infinity" security devices, video camera detectors, telephone privacy modules, subcarrier detectors, infra-red viewers, specialty microphones, audio jammers, tracking systems, telephone controllers, bullet-proof vests, gun hideaways, gas masks, chemical light sticks, countermeasure systems, specialty publications, and video surveillance equipment. $3.00 for a catalog. Address: Advanced Electronic Technologies, Suite 173, 5800-A N. Sharon Amity Rd., Charlotte, N.C., 28215.

Sherwood Communications Associates LTD. Product categories available: investigative aids, stealth, communications, video, van equipment, microphones, tape recorders, telephone accessories, telco tools, telephone recorders, monitoring, countermeasures, books, videos, and training materials. Address: Sherwood Communications Associates LTD, 1310 Industrial Highway, Southhampton, PA 18966. Phone: (215) 357-9065.

Gall's Inc. A catalog of products primarily for police and firemen: lightbars, gun and equipment holders, traffic movers, security items, traffic control, vehicle accessories, scanners, radios, antennas, flashlights, books, and handcuffs. Address: Gall's, P.O. Box 55268, 2470 Palumbo Dr., Lexington, KY 40555-5268. Phone: 800-524-4255. Fax: 606-269-4360.

Selective Books

Hackers. By Steven Levy. The history of hackers from 1960-1984 as heroes of the computer revolution. A dynamic book: well written, thoroughly interesting, and completely researched. Sometimes a bit hokey in making his "Hacker's Ethic" fit the circumstances, but overall a must read.

The Hacker's Handbook. By Hugo Cornwall. The first book specifically written for computer hackers. An excellent overall book, but technically lightweight when it comes to actually discussing hacking. ISBN 0-912579-06-4. Published by E. Arthur Brown Company: phone 612-762-8847.

Out of the Inner Circle. By Bill Landreth (now in its second edition). Bill Landreth was a member of a highly competent group of hackers before hacking became the latest rage. He was caught, convicted, sentenced, and lived to tell about it all in his book. ISBN 0-914845-36-5. Published by Microsoft Press.

The Computer Underground. By M. Harry. 20% good, 80% bad. Half the book contains old text files which have been around forever on the BBS circuit and are now obsolete. The book has its bright spots and chooses its subjects well, but is overall written poorly. Especially irritating is his incorrect analysis of mathematical chance and probabilities. ISBN 0-915179-31-8. Published by Loompanics Unlimited.

Die Hacker Bibel I & II. A bit of everything from the Chaos Computer club: some original material, news clipping, old *TAP* articles, Hackers Conference material, and computer art/humor. Over half of the material is written in German. ISBN 3-922708-98-6. Published by Der Grune. Also available through the Chaos Computer Club, Schwenckestr 85, D-2000 Hamburg 20, Germany.

The FBI and Your BBS. A guide for sysop's worried about legal security. 75% is fluff, 25% is the information the sysop needs to know. Published by The FBI Project. Phone (313) 747-7027.

The Cuckoo's Egg. By Clifford Stoll. This book has been in the news so much, any comments here would only by repetitious. ISBN 0-385-24946-2. Published by Doubleday.

Viruses

Computer Viruses, a High-Tech Disease. By Ralf

Burger. Bill Machrine, editor of *PC Magazine* described this book best: "...I've just seen what may be the most ill-conceived computer book ever. I can't bring myself to tell you the title, author, or publisher. This book about viruses strikes me as the height of opportunistic publishing and bad judgement.... Instead of a book offering a way to protect yourself against viruses...this is a how-to manual.... I knew this book had gone beyond the pale when I got to the chapters on attacking hardware, which included techniques for destroying monitors and disk drives...." ISBN 1-55755-043-3. Published by Abacus.

Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System. By John McAfee, Chairman of the Computer Virus Industry Association. A good book by someone who knows what viruses are. Covers all aspects of viruses: history, human factors, and computer considerations. Includes code for the more famous viruses. ISBN 0-312-03064-9. Published by St. Martin's Press.

Other worthy books mentioned briefly:

Computer Related Crime. All aspects superficially covered. Available from Loompanics.

Turing's Man. By J. David Botler.

Soul of a New Machine. By Tracy Kidder.

Neuromancer, Count Zero, Mona Lisa Overdrive, and *Burning Chrome.* All by William Gibson.

Unix System Security. By Robert Morris Senior. One of the best books on Unix security.

Computer Lib, 1987 Edition. By Ted Nelson. A counterculture computer book.

Computer Security Sources

(The majority of this list appeared in Computer Security Information Sources, by Russell Kay, *Computer Security Journal,* Volume IV, Number 1, pages 29-40.)

Computer Security Journal. Covers most topics as they relate to computer security, including software, hardware, and human factors. Published two times a year. $65 for a year ($60 for CSI members), 96 pages long. Address: Computer Security Institute, 360 Church Street, Northborough, MA 01532, phone (617) 393-2600.

Computers & Security. Aimed at the academic and technical oriented people. Published six times a year. $131.05 for a year. Address: Elsevier Journal Information Service, 52 Vanderbilt Avenue, New York NY 10017, phone (212) 916-1250.

Computer Security, Audit, and Control. Mostly brief digests of articles which have appeared in other magazines or newsletters, though it does contain some original material. Published 2 times a year. $55 for a year, around 60 pages per issue. Address: Management Advisory Publications, P.O. Box 151, Wellesley Hills, MA 02181, phone (617) 235-2895.

Data Processing & Communications Security. Covers a broad range of computer security subjects. Published four times a year. $30 for a year, 40 pages long. Address: Assets Protection, P.O. Box 5323, Madison, WI 53705, phone (608) 231-3817.

Internal Auditor. Discusses techniques of internal control and auditing. Published two times a month. $24 a year for non-members, free for members. Address: Institute of Internal Auditors, 249 Maitland Avenue, Altamonte Springs, FL 32701, phone (305) 830-7600.

Security (formerly *Security World*). For the loss prevention conscious person working in industrial or commercial areas. Published once a month. *freebie. Address: P.O. Box 5510, Denver, CO 80217, phone (303) 388-4511.

Security Management. For the manager in charge of security and preventing losses. Published once a month. $30 for a year, or included with an annual membership to the American Society for Industrial Security, it's $65 for the first time and then $55 to renew. Address: ASIS, 1655 N. Fort Meyer Drive, Suite 1200, Arlington, VA 22209, phone (703) 522-5800.

Security Systems Administration. For the person in charge of security, going over a wide range of topics, including retail. Published once a month. *freebie. Address: PTN Publishing Company, 201 Crossways Park Drive, Woodbury, NY 11797, phone (516) 496-8000.

Contingency Journal. The magazine for business planning. *freebie. Address: 10935 Estate Lane, Suite 375, Dallas, TX 75238, phone (214) 343-3717.

Telecommunications. Not about computers, but about telephones and network technology. Mentioned here because it's a *freebie. Address: 685 Canton Street, Norwood, MA 02062, phone (617) 769-9750.

Newsletters

Computer Crime Digest. Provides information relating to computer fraud and crimes. Published 12 times a year. $136 for a subscription, 10-12 pages long. Address: Washington Crime News Services, 7043 Wimsatt Rd, Springfield, VA 22151, phone (703) 941-6600.

Computer Fraud & Security Bulletin. Reports computer crime and how to prevent it. $240 for a subscription, 12 pages long. Address: Elsevier Journal Information Center, 52 Vanderbilt Ave., New York, NY 10164, phone (212) 916-1250.

Computer Law Newsletter. Covers all aspects of computer law and crime. Published twice a month. *freebie. Address: Warner & Stackpole, 28 State Street, Boston, MA 02109, phone (617) 951-9000.

Computer Security Newsletter. Discusses a wide range of subjects for the person in charge and responsible for computer security. Published twice a month. You must have a membership with the Computer Security Institute, $95 per year domestic, or $125 for overseas. 8 pages long. Address: Computer Security Institute, 360 Church Street, Northborough, MA 01532, phone (617) 393-2600.

HACKER LITERATURE

Computer Security Products Reports. Reviews computer security products. Published 4 times a year. $16 for a subscription. Address: Assets Protection, P.O. Box 5323, Madison, WI 53705, phone (608) 231-3817.

Computer/Law Journal. Discusses issues relating to computer law. Published quarterly. $76 for a year by the Center for Computer/Law, 112 Ocean Drive, Manhattan Beach, CA 90266.

Personal Identification News. For advanced access control technologies and practices, covering most devices and techniques. Published 11 times a year. $265 per year. Address: *Personal Identification News,* P.O. Box 11018, Washington DC, phone (202) 364-8586.

Privacy Journal. Reports all issues on personal privacy as affected by technology. Published monthly, 8 pages long. $89 for a year. Address: P.O. Box 15300, Washington, DC 20003, phone (202) 547-2865.

Security Letter. Their thrust is towards commercial and industrial security, stressing commercial security planning and physical security systems. Published twice a month. $137 for a year. Address: *Security Letter,* 166 East 96th Street, New York, NY 10128, phone (212) 348-1553.

Security Systems Digest. Keeps the reader up to date on the most recent developments in security systems for the commercial and industrial security practitioner. Published two times a week. $120 for a year, 10-12 pages. Address: Washington Crime News Services, 7043 Wimsatt Road, Springfield, WA 22151, phone (703) 941-6600.

Network Mailing Lists. To subscribe to a mailing list, send a message including your name and network address. There are over 250 mailing lists available covering a wage ranges of topics through the networks.

CERT. The Computer Emergency Response Team mailing list covering the latest virus attacks, discovered security holes, and appropriate patches. CERT.SEI.CUM.EDU

Computer Underground Digest. The best news available concerning the underground computer community. Covers most topics of interest to hackers. TK0JUT2@NIU.bitnet

ETHICS-L. Discussion of computer ethics. Usually generates more heat than light. Bitnet subscribers issue command: SUBSCRIBE ETHICS-L (your full name) to: LISTSERV@MARIST.BITNET

Other subscribers may write to: JROBINET%POLYTECH.BITNET@CUNYVM.CUNY.EDU

Fanzine. An electronic monthly science fiction magazine. fanzine %PLACI.SUN.COM

INFO-MODEMS. A discussion group of special interest to modem users. Info-Modems-Request@SIMTEL20.ARPA

INFO-UNIX. A question/answer forum for novice users, programmers, and administrators of the Unix operating system. INFO-UNIX-REQUEST@BRL.ARPA

INFO-VAX. Not to be outdone, the VMS operating system has its own forum for questions and answers. INFO-VAX-REQUEST@KL.SRI.COM

List of mailing lists. The current "list of lists" of mailing groups available. ZELLICH@SRI-NIC.ARPA

PACKET-RADIO. A discussion where people can exchange ideas about packet radio and discuss current projects. PACKET-RADIO-REQUESTS@EDDIE.MIT.EDU

RISKS. Distribution list for discussion of issues related to risks to the public in the use of computer systems. Sponsored by the ACM. RISKS-REQUEST@CSL.SRI.COM

SECURITY. Discusses all types of security. Most of the focus is on computers and locks of all sorts. SECURITY-REQUEST@AIM.RUTGERS.EDU

SF-LOVERS. A forum for science fiction fans of all topics. Bitnet subscribers issue the command: TELL LISTSERV at RUTMV1 SUBSCRIBE SFLOVERS (your full name). All others write to SF-LOVERS-REQUEST@RUTGERS.EDU

TELECOM. The best forum of all telephone related topics. Get this and your mailbox will never be empty again! eecs.new.edultelecom

Archives of telecom are available at lcs.mit.edu in the telecom-archives directory.

UNIX-WIZARDS. For people maintaining machines running the Unix operating system. UNIX-WIZARDS-REQUEST@BRL.ARPA

VIRUS-L. Forum specifically for the discussion of all topics of computer viruses. Bitnet subscribers issue the command: SUB VIRUS-L (your full name).

Other subscribers include the same command in the message body to: LISTSERV%LEHIIBM1.BITNET@MITVMA.MIT.EDU

2600 has meetings in New York and San Francisco on the first Friday of every month from 5 pm to 8 pm local time. See page 41 for specific details.

CLIP AND DISCARD

Central Office

This is one of the last articles to come out of The Legion of Doom
by Agent Steal

I should point out that the information in this article is correct to the best of my knowledge. I'm sure there are going to be people that disagree with me on some of it, particularly the references to tracing. However, I have been involved in telecommunications and computers for 12+ years.

I'm basing this article around the 1AESS since it is the most common switch in use.

Outside Plant

This is the wiring between your telephone and the central office. That is another article in itself so if you are interested read Phucked Agent 04's article on outside loop in the *LOD Technical Journal*. It explains those green boxes you see on street corners, aerial cables, manholes, etc. Where it stops, this article starts.

Cable Vault

All of the cables from other offices and from subscribers enter the central office underground. They enter into a room called the cable vault. This is a room generally in the basement located at one end or another of the building. The width of the room varies but runs the entire length of the building. Outside cables appear though holes in the wall. The cables then run up through holes in the ceiling to the frame room.

Understand that these cables consist of an average of 3600 pairs of wires. That's 3600 telephone line. The amount of cables obviously depends on the size of the office. All cables — interoffice, local lines, fiber optic, coaxial — enter through the cable vault.

Frame Room

The frame is where the cable separates to individual pairs and attaches to connectors. The frame runs the length of the building, from floor to ceiling. There are two sides to the frame, the horizontal side and the vertical side. The vertical side is where the outside wiring attaches and the protector fuses reside. The horizontal side is where the connectors to the switching system reside. Multi-conductor cables run from the connectors to actual switching equipment. So what we have is a large frame called the Main Distribution Frame (MDF) running the entire length of the building, floor to ceiling 5 feet thick. The MDF consists of two sides, the VDF and the HDF. Cables from outside connect on one side and cables from the switching equipment connect to the other. Jumper wires connect the two. This way any piece of equipment can be connected to any incoming "cable pair". These jumper wires are simply 2 conductor twisted pair running between the VDF and HDF.

What does all this mean? Well, if you had access to COSMOS you would see information regarding cable and pair and "OE" or originating equipment. With this you could find your line on the frame and on the switch. The VDF side is clearly marked by cable and pair at the top of the frame, however the HDF side is a little more complicated and varies in format from frame to frame and from one switch to another. Since I am writing this article around the 1AESS, I will describe the OE format used for that switch.

OE ABB-CDD-EFF where: A = Control group (when more than one switch exists in that C.O.); B = LN Line Link Network; C = LS Line Switching Frame; D = CONC or concentrator; E = Switch (individual, not the big one); F = Level. There is one more frame designation called LOC or location. This gives the location of the connector block on the HDF side.

Switching Systems

Writing an article that covers them all would be lengthy indeed. So I am only going to list the major ones and a brief description of each.

Step by Step (Strowger 1889). First automatic, required no operators for local

calls, no custom calling or touch tone, manufactured by many different companies in different versions, hard wire routing instructions, could not chose an alternate route if programmed route was busy. Each dial pulse tripped a "stepper" type relay to find its path.

No. 1 Crossbar (1930); - No. 5 Crossbar (1947) (faster, more capacity). Western Electric, first ability to find idle trunks for call routing, no custom calling or equal access, utilized a 10x20 cross point relay switches, hard wired common control logic for program control, also copied by other manufacturers.

No. 4 Crossbar. Used as a toll switch for AT&T's long line network, 4-wire tandem switching, not usually used for local loop switching.

No. 1ESS (1966); - No. 1AESS (1973). Western Electric, described in detail later in file.

No. 1EAX. GTE Automatic Electric, GTE's version of the 1AEES, slower and louder.

No. 2ESS (1967); - No. 2BESS (1974). Western Electric, analog switching under digital control, very similar to the No. 1ESS and No. 1AESS, downsized for smaller applications.

No. 3ESS. Western Electric, analog switching under digital control, even smaller version of No. 1AESS, rural applications up to 4500 lines.

No. 2EAX. GTE Automatic Electric, smaller version of 1EAX, analog switch under digital control.

No. 4ESS. Western Electric, toll switch, 4-wire tandem, digital switching, uses the 1AESS processor.

No. 3EAX. Gee, is there a pattern here? No, GTE. Digital toll switch, 4-wire tandem switching.

No. 5ESS. AT&T Network Systems, full scale computerized digital switching, ISDN compatibility, utilizes time sharing technology, toll or end office.

DMS 100 Digital Matrix Switch. Northern Telecom, similar to 5ESS, runs slower, considerably less expensive.

DMS 200. Toll and Access Tandem, optional operator services.

DMS 250. Toll switch designed for common carriers.

DMS 300. Toll switch for international gateways.

No. 5EAX. GTE Automatic Electric, same as 5ESS.

How much does a switch cost? A fully equipped 5ESS for a 40,000 subscriber end office can cost well over 3 million dollars. Now you know why your phone bill is so much. Well... maybe your parent's bill.

The 1ESS and 1AESS

This was the first switch of its type placed into widespread use by Bell. Primarily an analog switch under digital control, the switch is no longer being manufactured. The 1ESS has been replaced by the 5ESS and other full scale digital switches. However, it is still by far the most common switch used in today's class 5 end offices.

The #1 and 1A use a crosspoint switching matrix similar to the crossbar. The primary switch used in the matrix is the fereed (remreed in the 1A). It is a two-state magnetic alloy switch. It is basically a magnetic switch that does not require voltage to stay in its present position. Voltage is only required to change the state of the switch.

The #1 utilized a computer style common control and memory. Memory used by the #1 changed with technology, but most have been upgraded to RAM. Line scanners monitor the status of customer lines, crosspoint switches, and all internal, outgoing, and incoming trunks, reporting their status to the central control. The central control then either calls upon program or call store memories to choose which crosspoints to activate for processing the call. The crosspoint matrixes are controlled via central pulse distributors which in turn are controlled by the central control via data buses. All of the scanners, AMA tape controllers, pulse distributors, x-

point matrix, etc., listen to data buses for their address and command or report their information on the buses. The buses are merely cables connecting the different units to the central control.

The 1E was quickly replaced by the 1A due to advances in technology. So 1A's are more common. Also, many of the 1E's have been upgraded to 1A's. This meant changing the fereed to the remreed relay, adding additional peripheral component controllers (to free up central controller load) and implementation of the 1A processor. The 1A processor replaced older style electronics with integrated circuits. Both switches operate similarly. The primary differences were speed and capacity. The #1ESS could process 110,000 calls per hour and serve 128,000,000 lines.

Most of the major common control elements are either fully or partially duplicated to ensure reliability. Systems run simultaneously and are checked against each other for errors. When a problem occurs the system will doublecheck, reroute, or switch over to auxiliary to continue system operation. Alarms are also reported to the maintenance console and are in turn printed out on a printer near the control console.

Operation of the switch is done through the Master Control Center (MCC) panel and/or a terminal. Remote operation is also done through input/output channels. These channels have different functions and therefore receive different types of output messages and have different abilities as far as what type of commands they are allowed to issue. Here is a list of the commonly used TTY channels.

Maintenance: Primary channels for testing, enable, disable, etc.

Recent Change: Changes in class of service, calling features, etc.

Administrative: Traffic information and control.

Supplementary: Traffic information supplied to automatic network control.

SCC Maint: Switching control centers interface.

Plant Service Center: Reports testing information to test facilities.

At the end of this article you will find a list of the most frequently seen Maintenance channel output messages and a brief description of their meanings. You will also find a list of frequently used input messages.

There are other channels as well as backups but the only ones to be concerned with are Recent Change and SCC Maint. These are the two channels you will most likely want to get access to. The Maintenance channel doesn't leave the C.O. and is used by switch engineers as the primary way of controlling the switch. During off hours and weekends the control of the switch is transferred to the SCC.

The SCC is a centrally located bureau that has up to 16 switches reporting to it via their SCC maint. channel. The SCC has a mini-computer running SCCS that watches the output of all these switches for trouble conditions that require immediate attention. The SCC personnel then has the ability to input messages to that particular switch to try and correct the problem. If necessary, someone will be dispatched to the C.O. to correct the problem. I should also mention that the SCC mini has dialups and access to SCCS means access to all of the switches connected to it.

The Recent Change channels also connect to a centrally located bureau referred to as RCMAC. These bureaus are responsible for activating lines, changing class of service, etc. RCMAC has been automated to a large degree by computer systems that log into COSMOS and look for pending orders. COSMOS is basically an order placement and record keeping system for central office equipment, but you should know that already, right? So this system called MIZAR logs into COSMOS, pulls orders requiring recent change work, then in one batch several times a day, transmits the orders to the appropriate

Central Office Tick

switch via its Recent Change Channel.

Testing of the switch is done by many different methods. Bell Labs has developed a number of systems, many accomplishing the same functions. I will only attempt to cover the ones I know fairly well.

The primary testing system consists of the trunk test panels located at the switch itself. There are three and they all pretty much do the same thing: test trunk and line paths through the switch.

Trunk and Line Test Panel
Supplementary Trunk Test Panel
Manual Trunk Test Panel

MLT Mechanized Loop Testing is another popular one. This system, often available through the LMOS database, can give very specific measurements of line levels and losses. The "TV Mask" is also popular giving the user the ability to monitor lines via a call back number.

DAMT Direct Access Mechanized Testing is used by line repairman to put tone on numbers to help them find lines. This was previously done by Frame personnel, so this automated that task. DAMT can also monitor lines, however the audio is scrambled in a manner that allows one only to tell what type of signal is present on the line, or whether it is busy or not.

All of these testing systems have one thing in common. They access the line through a "No Test Trunk". This is a relay (in the 1ESS) which can drop in on a specific path or line and connect it to the testing device. The test trunks are part of the switch itself and act like a telephone line into the switch. The function of this line is strictly for access and testing of subscriber lines. It depends on the device connected to the trunk, but there is usually a noticeable click heard on the tested line when the No Test Trunk drops in. Also the testing devices I have mentioned here will seize the line, busying it out. This will present problems when trying to monitor calls — you would need to drop in on calls in progress. The No Test Trunk is also the method in which operator consoles do verifications and interrupts.

Interoffice Signalling

Calls coming into and leaving the switch are routed via trunks. The switches select which trunk will route the call most effectively and then retransmits the dialed number to the distant switch. There are several different ways this is done. The two most common are Loop Signaling and CCIS, Common Channel Interoffice Signaling. The predecessor to both of these is the famous and almost extinct "SF Signaling". This utilized the presence of 2600 hz to indicate trunk in use. If one winks 2600 hz down one of these trunks, the distant switch would think you hung up. Remove the 2600, and you have control of the trunk and you could then MF your own number. This worked great for years. Assuming you had dialed a toll-free number to begin with, there was no billing generated at all. The 1AESS does have a program called SIGI that looks for any 2600 winks after the original connection of a toll call. It then proceeds to record on AMA and output any MF digits received. However due to many long distant carriers using signaling that can generate these messages it is often overlooked and "SIG IRR" output messages are quite common.

Loop signaling still uses MF to transmit the called number to the distant switch. However, the polarity of the voltage on the trunk is reversed to indicate trunk use.

CCIS, sometimes referred to as CCS#6, uses a separate data link sending packets of data containing information regarding outgoing calls. The distant switch monitors the information and connects the correct trunk to the correct path. This is a faster and more efficient way of call processing and is being implemented all over. The protocol that AT&T uses is CCS7 and is currently being accepted as the industry standard. CCS6 and CCS7 are somewhat similar.

Interoffice trunks are multiplexed together onto one pair. The standard is 24

(continued on page 18)

ATTACHMENT 1

"CLASSIFICATIONS"

Definitions and Examples of Discourteous Actions Which Warrant Discipline:

1. NOT BUSINESSLIKE:

Definition: Not exhibiting tone and manner felt to be appropriate in business - e.g., talking in a joking or jesting manner at inappropriate times. Use of slang - non-standard vocabulary.

Example: Customer: "I would like to call person to person the Sales Manager."

Operator: "Got ya." "Does he have a name and gimme the number."

or

"Oh, calling a big shot today."

2. RUDE, ANTAGONISTIC, ABUSIVE:

Definition: Offensive in manner or action. Ill-mannered, abrupt, forceful, argumentative, impatient, sarcastic, cutting. To provoke hostility, abuse verbally.

Example: Customer: "Operator, did you say the Area Code was 213 or 212?"

Operator: "The trouble with you is you don't listen." "I'll tell you once more 2-1-2 and don't ask again."

or

"Can't you understand English?" "I said 2-1-2!"

Example: Customer: "When am I going to get my number, Operator?"

Operator: "Never if I had any say about it." "If you weren't so dumb you could dial it yourself."

or

"When I feel like it." "Don't rush me."

documents

3. SWEARING, VULGAR:

A. Profane:

Definition: To use profanity. To debase by wrong, unworthy or vulgar statements. Irreverent.

Customer: "Hey, operator where have you been out to coffee?" "I'm ready for another call."

Operator: "Just one damn minute." "Who the hell do you think you are, someone special?" "Anyway it's none of your G.D. business."

or

"Customers like you give me a pain - you know where."

B. Obscene:

Definition: Disgusting, repulsive, dirty, foul, nasty, vile, unprintable.

Example: Customer: "You connected me with a wrong number, now try it again."

Operator: "Oh, sh--, customers like you frost my a--."

or

"Tough, kiss my a--."

The above examples are intended to be the mildest description of each category.

THIS COMES FROM AN UNNAMED PHONE COMPANY'S MANUAL FOR SUPERVISORS. DOESN'T IT JUST FROST YOUR A--?

(continued from page 15)

channels per pair. This is called T-1 in its analog format and D-1 in its digital format. This is often referred to as carrier or CXR. The terms frame error and phase jitter are part of this technology which is often a world in itself. This type of transmission is effective for only a few miles on twisted pair. It is often common to see interoffice repeaters in manholes or special huts. Repeaters can also be found within C.O.'s, amplifying trunks between offices. This equipment is usually handled by the "carrier" room, often on another floor. Carrier also handles special circuits, private lines, and foreign exchange circuits.

After a call reaches a Toll Switch, the transmit and receive paths of the calling and called party are separated and transmitted on separate channels. This allows better transmission results and allows more calls to be placed on any given trunk. This is referred to as 4 wire switching. This also explains why during a call, one person can hear crosstalk and the other can't. Crosstalk is bleed-over from other channels on the multiplexed T-Carrier transmission lines used between switches.

Call Tracing

So with loop signaling standard format there is no information being transmitted regarding the calling number between switches. This therefore causes the call tracing routine to be at least a two-step method. This is assuming you are trying to trace an anticipated call, not one in progress. When call trace "CLID" is placed on a number, a message is output every time someone calls that number. The message shows up on most of the ESS output channels and gives information regarding the time and the number of the incoming trunk group. If the call came from within that office, then the calling number is printed in the message. Once the trunk group is known, it can usually be determined what C.O. the calls are coming from. This is also assuming that the calls are coming from within that Bell company and not through a long distance carrier (IEC). So if Bell knows what C.O. the calls are coming from, they simply put the called number on the C.I. list of that C.O. Anytime anyone in that C.O. calls the number in question another message is generated showing all the pertinent information.

Now if this were a real time trace, it would only require the assistance of the SCC and a few commands sent to the appropriate switches (i.e. NET-LINE). This would give them the path and trunk group numbers of the call in progress. Naturally the more things the call is going through, the more people will need to be involved in the trace. There seems to be a common misconception about the ability to trace a call through some of the larger packet networks like Telenet. Well, I can assure you, Telenet can track a call through their network in seconds and all that is needed is the cooperation of the Bell companies. Call tracing in itself is not that difficult these days. What is difficult is getting the different organizations together to cooperate. You have to be doing something relatively serious to warrant tracing in most cases, however, not always. So if tracing is a concern, I would recommend using as many different companies at one time as you think is necessary, especially US Sprint. They can't even bill people on time much less trace a call.

Equal Access

The first thing you need to understand is that every IEC (Inter Exchange Carrier) — or long distance company — needs to have an agreement with every LEC (Local Exchange Carrier) — or your local phone company — that they want to have access to and from. They have to pay the LEC for the type of service they receive and the amount of trunks, and trunk use. The cost is high and the market is a zoo. The LECs have the following options.

Feature Group A: This was the first access form offered to the IECs by the LECs. Basically whenever you access an IEC by dialing a regular 7 digit number (POTS line), this is FGA. The IEC's

equipment would answer the line, interpret your digits, and route your call over their own network. Then they would pick up an outgoing telephone line in the city you were calling and dial your number locally. Basically a dial in, dial out situation similar to PC Pursuit.

Feature Group B: FGB is 950-xxxx. This is a very different setup from FGA. When you dial 950, your local switch routes the call to the closest Access Tandem (Toll Switch) in your area. There the IECs have direct trunks connected between the AT and their equipment. These trunks usually use a form of multiplexing like T-1 carrier with wink start (2600hz). On the incoming side, calls coming in from the IEC are basically connected the same way. The IEC MFs into the AT and the AT then connects the calls. There are a lot of different ways FGB is technically set up, but this is the most common.

Tracing on 950 calls has been an area of controversy and I would like to clear it up. The answer is yes, it is possible. But like I mentioned earlier, it would take considerable manpower which equals expensive to do this. It also really depends on how the IEC interface is set up. Many IECs have trunks going directly to class 5 end offices. So, if you are using a small IEC, and they figure out what C.O. you are calling from, it wouldn't be out of the question to put CLID on the 950 number. This is highly unlikely and I have not heard from reliable sources of it ever being done. Remember, CLID generates a message every time a call is placed to that number. Excessive call trace messages can crash a switch. However, I should mention that brute force hacking of 950s is easily detected and relatively easy to trace. If the IEC is really having a problem in a particular area, they will pursue it.

Feature Group C: FGC is reserved for and used exclusively by AT&T.

Feature Group D: FGD is similar to FGB with the exception that ANI is MFed to the IEC. The end office switch must have Equal Access capability in order to transmit the ANI. Anything above a crossbar can have it. I guess I should mention that it is possible for a crossbar to have it with modifications. FGD can only be implemented on 800 numbers and if an IEC wants it, they have to buy the whole prefix. You should also be aware that long distance companies offer a service where they will transmit the ANI to the customer as well. You will find this being used as a security or marketing tool by an increasing amount of companies. A good example would be 800-999-CHAT.

1AESS Common Output Messages

(Message is followed by a description.)

Alarm

AR01: Office alarm
AR02: Alarm retired or transferred
AR03: Fuse blown
AR04: Unknown alarm scan point activated
AR05: Commercial power failure
AR06: Switchroom alarm via alarm grid
AR07: Power plant alarm
AR08: Alarm circuit battery loss
AR09: AMA bus fuse blown
AR10: Alarm configuration has been changed (retired, inhibited)
AR11: Power converter trouble
AR13: Carrier group alarm
AR15: Hourly report on building and power alarms

Automatic Trunk Test

AT01: Results of trunk test

Carrier Group

CG01: Carrier group in alarm
CG03: Reason for above

Coin Phone

CN02: List of pay phones with coin disposal problems
CN03: Possible Trouble
CN04: Phone taken out of restored service because of possible coin fraud

Copy

COPY: Data copied from one address to another

Call Trace

CT01: Manually requested trace line to line, information follows

CT02: Manually requested trace line to trunk, information follows
CT03: Intraoffice called placed to a number with CLID
CT04: Interoffice called placed to a number with CLID
CT05: Call placed to number on the CI list
CT06: Contents of the CI list
CT07: ACD related trace
CT08: ACD related trace
CT09: ACD related trace

Digital Carrier Trunk

DCT COUNTS: Count of T carrier errors

Memory Diagnostics

DGN: Memory failure in cs/ps diagnostic program

Digital Carrier "Frame" Errors

FM01: DCT alarm activated or retired
FM02: Possible failure of entire bank, not just frame
FM03: Error rate of specified digroup
FM04: Digroup out of frame more than indicated
FM05: Operation or release of the loop terminal relay
FM06: Result of digroup circuit diagnostics
FM07: Carrier group alarm status of specific group
FM08: Carrier group alarm count for digroup
FM09: Hourly report of carrier group alarms
FM10: Public switched digital capacity failure
FM11: PUC counts of carrier group errors

Maintenance

MA02: Status requested, print out of MACII scratch pad
MA03: Hourly report of system circuits and units in trouble
MA04: Reports condition of system
MA05: Maintenance interrupt count for last hour
MA06: Scanners, network, and signal distributors in trouble
MA07: Successful switch of duplicated unit (program store etc.)
MA08: Excessive error rate of named unit
MA09: Power should not be removed from named unit
MA10: OK to remove paper
MA11: Power manually removed from unit
MA12: Power restored to unit
MA13: Indicates central control active
MA15: Hourly report of number of times interrupt recovery program acted
MA17: Centrex data link power removed
MA21: Reports action taken on MAC-REX command
MA23: 4 min. report, emerg. action phase triggers are inhibited

Memory

MN02: List of circuits in trouble in memory

Network Trouble

NT01: Network frame unable to switch off line after fault detection
NT02: Network path trouble Trunk to Line
NT03: Network path trouble Line to Line
NT04: Network path trouble Trunk to Trunk
NT06: Hourly report of network frames made busy
NT10: Network path failed to restore

Operating System Status

OP:APS-0
OP:APSTATUS
OP:CHAN
OP:CISRC: Source of critical alarm, automatic every 15 minutes
OP:CSSTATUS: Call store status
OP:DUSTATUS: Data unit status
OP:ERAPDATA: Error analysis database output
OP:INHINT: Hourly report of inhibited devices
OP:LIBSTAT: List of active library programs
OP:OOSUNITS: Units out of service
OP:PSSTATUS: Program store status

Plant Measurements

PM01: Daily report
PM02: Monthly report
PM03: Response to a request for a specific section of report
PM04: Daily summary of IC/IEC irregularities

Report

REPT:ADS FUNCTION: Reports that an ADS function is about to occur
REPT:ADS FUNCTION DUPLEX FAILED:

# of a Central Office

No ADS assigned
REPT:ADS FUNCTION SIMPLEX: Only one tape drive is assigned
REPT:ADS FUNCTION STATE CHANGE: Change in state of ADS
REPT:ADS PROCEDURAL ERROR: You fucked up
REPT:LINE TRBL: Too many permanent off hooks, may indicate bad cable
REPT:PROG CONT OFF-NORMAL: System programs that are off or on
REPT:RC CENSUS: Hourly report on recent changes
REPT:RC SOURCE: Recent change system status (RCS=1 means RC Chan. inhibited)

Recent Change

RC18: RC message response

Remove

RMV: Removed from service

Restore

RST: Restored to service status

Ringing and Tone Plant

RT04: Status of monitors

Software Audit

SA01: Call store memory audit results
SA03: Call store memory audit results

Signal Irregularity

SIG IRR: Blue box detection
SIG IRR INHIBITED: Detector off
SIG IRR TRAF: Half hour report of traffic data

Traffic Condition

TC15: Reports overall traffic condition
TL02: Reason test position test was denied
TL03: Same as above

Trunk Network

TN01: Trunk diagnostic found trouble
TN02: Dial tone delay alarm failure
TN04: Trunk diag request from test panel
TN05: Trunk test procedural report or denials
TN06: Trunk stat change
TN07: Response to a trunk type and status request
TN08: Failed incoming or outgoing call
TN09: Network relay failures
TN10: Response to TRK-LIST input, usually a request from test position
TN11: Hourly, status of trunk undergoing tests
TN16: Daily summary of precut trunk groups

Traffic Overload Condition

TOC01: Serious traffic condition
TOC02: Reports status of less serious overload conditions

Translation (shows class of service, calling features, etc.)

TR01: Translation information, response to VFY-DN
TR03: Translation information, response to VFY-LEN
TR75: Translation information, response to VF:DNSVY
TW02: Dump of octal contents of memory

1AESS Common Input Messages

Messages always terminate with ". ctrl d ",
x=number or trunk network #

NET-LINE-xxxxxxx0000: Trace of path through switch
NET-TNN-xxxxxx: Same as above for trunk trace
T-DN-MBxxxxxxx: Makes a # busy
TR-DEACTT-26xxxxxxx: Deactivates call forwarding
VFY-DNxxxxxxx: Displays class of service, calling features etc.
VFY-LENxxxxxxxx: Same as above for OE
VFY-LIST-09 xxxxxxx: Displays speed calling 8 list

***

There are many things I didn't cover in this article and many of the things I covered, I did so very briefly. My intention was to write an article that explains the big picture, how everything fits together. I hope I helped.

Special thanks to all the stupid people, for without them some of us wouldn't be so smart and might have to work for a living. Also special thanks to John and Dave for without their guidance, this would have never been written. Yes, people, there are great hackers out there that no one has ever heard of. You just have to know where to find them.

anatomy of

In our last issue, you may have noticed a reference to a service called 1-900-STOPPER on pages 25-26 that allows you to place a call without being Caller-ID'd for $2 a minute. We referred to it as "another rip-off that preys on people's fears." We also said it didn't allow you to call 800 numbers which frequently identify the numbers of their callers.

It looks like we ruffled some feathers. The following letter was sent to us by Will Dwyer, President and CEO of Private Lines, Inc. and a copy sent to their lawyer, M.L. Rudnick:

"Having gained knowledge yesterday of your having published in the Autumn 1990 issue of *2600 Magazine* (pages 25-26) that our telephone service, which you characterize as 'another rip-off,' 'won't allow you to call 800 numbers,' we hereby (1) serve notice on you of our claim that your statement is libelous and (2) demand that it be corrected. (Section 48a, Civil Code of California.)

"Had you either inquired of us or tried the service yourself, you would have found that a caller can reach an 800 number — without transmitting ANI (automatic number identification) for his or her phone number — via the same procedure by which our 1-900-STOPPER (786-7737) service allows call completion to any other U.S. telephone number. (Your writer, 'EH,' should have noted that the $2 per minute applies to calls anywhere in the U.S., not 'just local.' The $5 per minute service is a separate one for international calls; access to it is via 1-900-RUN WELL (786-9355)."

In a typical issue of *2600,* we point out quite a few discrepancies, inequities, or rip-offs. In each case we have specific knowledge which leads us to our conclusions. In this particular instance, we were replying to a letter ("EH" wrote the letter and is not one of our writers). We believed at the time, and we still do, that our assessment was correct.

This attempt to intimidate us into taking back our words does nothing but infuriate us. We have an obligation to be honest and open with our readers and no one person, company, or governmental agency will convince us to betray or suppress that trust.

Let's take a closer look at 1-900-STOPPER. We first tried calling 800 numbers through their service months ago. It didn't work. It still doesn't. We challenge anyone to use this service to make an 800 call to MCI (800-444-4444) or the Runaway Hotline (800-999-9999) or *any* 800 number. We did finally find one that worked, (AT&T: 800-222-0300). But the majority we tried didn't. We got a fast busy signal indicating some kind of a restriction.

Out of fairness, we cannot say that the service doesn't connect to 800 numbers. It does, sometimes. But one thing the service did do consistently was bill us for every attempt we made. Which brings us to the word "rip-off". A service that bills customers for absolutely nothing is, in our opinion, a very good example of this. If you use 1-

a rip-off

900-STOPPER to connect to a number that's busy, you'll still get billed $2 for the attempt.

Even if the system worked perfectly and only billed for the actual time connected, we still find its premise absurd. $2 a minute to make a local call or toll-free call? (There would be little need to use the service to dial nationally since there is currently no form of caller identification in place for long distance calls. Caller ID is only used locally and ANI is only used on toll-free calls, at least for the moment. It's true that there would be no long distance phone bill linked to the caller but if he/she were under surveillance, the digits they dialed would still show up on a pen register.)

As for this other service (1-900-RUN WELL), we find $5 a minute an obscene amount to charge for a phone call to anywhere. And what kind of privacy is being guaranteed here? Any international call is still subject to monitoring by the NSA. Your phone could still be tapped. A pen register could still be on your line. There is no international Caller ID or ANI to avoid.

We tried this service as well and found it disturbing. There was no mention at all of the high price. (Perhaps this helps explain why our letter writer got the pricing wrong.) All we were told was to enter the international number we wanted to call. We got a recording from AT&T saying all circuits were busy as well as a sinking feeling that we were going to get charged $5 for the privilege of hearing that bit of information.

Do we have anything at all good to say about these two services? Yes. It's good to recognize the right to privacy and let people know they don't have to be constantly monitored. There should always be alternatives to that. But, for the reasons given, we find these particular alternatives to be wholly inadequate ones.

Itemized calls, continued

Directly dialed

No.	Date	Place called	Number called	Time	Rate	Min.	Amount
		UK	4481	5 14 PM	DD	28	20.32
		NETHERLAND	3120	5 44 PM	DD	1	1.35
		MULTIQUEST	900 786-7737	4 51 AM		1	2.00
		MULTIQUEST	900 786-7737	4 40 PM		1	2.00
		MULTIQUEST	900 786-7737	4 41 PM		1	2.00
		MULTIQUEST	900 786-7737	4 42 PM		1	2.00
		MULTIQUEST	900 786-7737	4 43 PM		2	4.00
		MULTIQUEST	900 786-7737	4 45 PM		1	2.00
		NETHERLAND	3120	1 16 PM	DD	3	2.95
		SAUDI ARAB	9663	5 32 PM	DD	3	4.11
		GER FED RP	4930	2 16 PM	DD	1	1.42

Only the last attempt resulted in a successful call completion. But that didn't stop these wonderful people from billing us anyway.

IT'S THE

COCOT Troubles

Dear 2600:

I am presently enrolled in a senior high school in Fayetteville, NC. This school is robbing its students blind by having two COCOTs in the lobby. I obtained a copy of *2600* through a friend and I am interested in receiving more. Furthermore, I would like to request some extra information in hacking out these COCOTs so that I can get free LD's. My friend noted that these phones used a hangup pulse that hung up the phone when it read zero volts on the line. So he hooked in a nine volt battery in parallel until the number connected. I want to see if there are other less difficult ways of hacking this phone.

KM

By all means figure out how the phone works, but if all you're interested in is making free phone calls, you're not a whole lot better than the sleazoids who installed the phone in the first place. See what happens after the called party hangs up. Do you by chance get an unrestricted dial tone on your end? Look for speed dials that are programmed in via the star or pound keys. And see what happens when you call it. We suggest reading The Plague's COCOT article (Summer 1990).

Future Surveillance

Dear 2600:

The article "New Revelations from BellSouth" (by Emmanuel Goldstein, Autumn 1990) describes new monitoring technology. From this description, it appears to be a well-designed system for performing such monitoring. The author appears to believe that BellSouth should have improved their security in a different way.

However, wasn't the goal of some of the attacks against various Bell computers to demonstrate that Bell should improve their security? Why, then, the objection when they actually do so? And shouldn't they be free to select the method that they use?

fin
Minnesota

Not when that method carries extremely troubling implications. Note that the monitoring device BellSouth is interested in is capable of far more than "improving security". It can watch a variety of lines simultaneously, recording voice, fax, and computer transmissions automatically. Its configuration leads one to the conclusion that any interested entity will be able to monitor an individual thoroughly, even without the phone company's knowledge or approval. That's something none of us will be served by.

Why Did You Do It?

Dear 2600:

I was disappointed to see that you published the credit card algorithm in your Fall 1990 issue.

Although I know it was well within your First Amendment rights to publish it, I think that it serves no purpose by being published except to leave innocent credit card holders open to abuse by individuals who just wish to call a phone sex line or place a long distance call over an AOS. And although I know that the algorithm was already well known within the hacker world, I don't believe that your magazine should have spread it further.

In previous issues of *2600*, you stated that credit card fraud and long distance code abuse are tantamount to stealing and have nothing to do with the hacker ethic of learning and exploring systems. Therefore, I see no reason to publish the credit card algorithm if your magazine truly believes in the above. The only uses of the credit card algorithm by your readers would be to generate numbers to be used to place calls over an AOS, access to phone sex lines or 800 chat lines which use credit card numbers for billing, or to obtain actual merchandise as the authors of your article state that often credit card numbers are often checked only against the algorithm and then billed later.

Please stick to your ideals. If you believe that credit card fraud and code abuse are stealing and not hacking, then please do not publish any information that would be used to those ends. And please try not to publish materials from authors who call themselves names such as "K00l/RaD Alliance!". Your mag will end up looking like a "s00per-elYte c0dez phile!".

Questmaster
Santa Barbara, CA

You raise good points, but you've missed the point of 2600. We published that information so people would understand how the technology worked. What they do with that information is not our business. Read on

LETTERS PAGE

for another opinion.

Dear 2600:

In the article "An Algorithm For Credit Cards", there was an error in the C code that caused the program to incorrectly determine the weighting factor for 13 digit Visa cards. Here is a correct version, as employed in the form of a function:

```
is_valid_cc(kind, card_number)
int kind;
char *card_number;
{
  char ccn[30];
  int validP = 0;
  int cclen = 0, llen = 0;
  int cdigit = 0, csum = 0;

    cclen = strlen(strncpy(&ccn,
card_number, 30));

  /* is this the right length for this
kind of card? */
  switch(kind) {
  case VISA:
    if (((cclen != 13) && (cclen != 16)) ||
(ccn[0] != '4'))
      return(0);
    break;
  case MC:
    if ((cclen != 16) || (ccn[0] != '5'))
      return(0);
    break;
  case AMEX:
    if ((cclen != 15) || (ccn[0] != '3'))
      return(0);
    break;
  default:
    return(0);
  }

  for (llen=0; llen < cclen; llen++) {
    cdigit = ccn[llen] - '0';
    if ((llen + 1) % 2) cdigit *= 2;
    if (cdigit >= 10) cdigit -= 9;
    csum += cdigit;
  }
  if ((csum % 10) == 0) return(1);
  return(0);
}
```

This function will return 0 if incorrect, 1 if correct. "VISA", "MC" and "AMEX" are arbitrarily defined constants, and may be ignored.

Thank you for including this article — we have needed something to keep people from 'fumble-fingering' on card entries.

Kenton A. Hoover
Chief Engineer
Whole Earth Lectronic Link

Questions

Dear 2600:

I very much enjoy your magazine and I am curious whether certain companies tell the federal government or the phone companies the names of people that send away for crystals to make a red box.

Also, please print the frequencies of each touch tone. I'm writing melodies with them.

Rob
Woodmere, NY

It's not beyond the realm of possibility that some companies do that. The solution is to do what appeals to you and not worry about what others think, whether they be ignorant people or malignant bureaucracies. Touch tones are comprised of two frequencies each. Picture your touch tone keypad, with the extra A-B-C-D column on the right. Then place the following frequencies along the top: 1209 hz, 1336 hz, 1477 hz, and 1633 hz. From top to bottom the frequencies are: 697 hz, 770 hz, 852 hz, and 941 hz. Find the number you want and combine the two tones for that number and you've got a touch tone!

BBS Troubles

Dear 2600:

I have recently read the two articles about the E911 case that were published in the Spring 1990 edition of your magazine. First of all, I want to thank you for bringing things like these into the open. The federal government is always trying to keep their misconduct (which occurs all too often) under their hats, and it's great to see that people still have the guts to stand up to it.

I have also been feeling the effects of these "crackdowns" here in the Twin Cities. Many a BBS have disappeared (along with their operators). Many more have been looked into, but allowed to remain. Almost every BBS in the state now posts a warning message about the "privacy" of e-mail. I feel sorry for one BBS in particular: Hotline. It was clearly known to everyone that this BBS was completely legitimate. Yet, recently, they were the subject of a federal investigation. Apparently they had a set of users that were referred to as "privileged users". Someone who was uninformed and didn't take the

time to look into things further assumed that the "privileged users" were hackers and received access to some secret part of the BBS. Actually, a "privileged user" is someone who contributes money to the BBS and receives privileges such as more online time, extra downloads, etc. The operators have since changed the status to "contributors" rather than "privileged users" to avoid future confusion. It is hard to believe that this anti-hacker paranoia has grown to such proportions that people even get harassed for merely contributing money to a BBS that they like. In any case, I'm glad to see that this board, as well as many others, has survived the attacks and has the pride, determination, caring, and guts to remain in operation.

Finally, since my interest in cases such as these has grown recently, I would like to know what else is going on. Here in the Twin Cities, I have been waging a battle of my own: against censorship. I am concerned about how successful the PMRC (Parent Music Resource Center) has been in limiting the rights of musicians to say what they feel. Also, I feel that hackers are not doing anything that would cause harm to anyone, and should also be guaranteed the right to the First Amendment. I would like to receive more information about your magazine and how I may subscribe to it. I want to assure you that I am not a federal agent, nor do I have any contacts with the federal government. I am not interested in busting you or your magazine, but simply in learning more about what is going on.

The Spectre
St. Paul, MN

It wouldn't matter if you were. We provide the same information to anyone who's interested. We hope to see hacker bulletin boards recover from what has been a crippling blow. There are a great deal that are truly underground now. The need for public hacker boards has never been greater. Anyone who has questions about this should contact us.

Dear 2600:

I have been hearing rumors that the Federal Communications Commission is going to begin forcing BBS sysops to keep printed logs of their BBS's up to three years back. As a BBS sysop, I find it good practice to keep my logs, but after all of the work I've put into the board, I don't want the government telling me what I should do with it!

Charlie Tuna
Kokomo, IN

This is only one of the many pressures being put on system operators. Another is the threat of charging business phone rates to bulletin boards, an action that would put many of them out of existence. Counter these threats by uniting with your users and other system operators. And by sending letters to major publications like us.

Another Method

Dear 2600:

I just received your Autumn 1990 issue and, like always, I read it cover to cover. Very enjoyable and entertaining. I am involved with modifying scanners to get cellular, reprogramming cellular phones (for the obvious reasons), data reception from satellites, and just about anything else that is beyond the normal grasp. I have the programming procedure for over 45 cellular phones and a complete listing of tower codes for all states, several COCOT payphone manuals, and wiring diagrams. Between your magazine and the URR Newsletter, I get lots of ideas. For your readers that don't know, URR Newsletter sells lots of unusual parts and plans. I have been a fan of theirs for years. I got my start in CBs and progressed from there. Just thought I would let you know that I appreciate your existence.

Now for the good stuff. Recently I found a COCOT that had the serial numbers on the lock mechanisms. It don't get any easier than that. After opening the phone I discovered a programming switch inside. Now I can remove the static ram to dump the passwords and, to my delight, I now have an operating payphone. Just for fun, I left it in the same location, with the passwords changed of course. I'm really not into theft. I just like to explore. Bin 99 holds the programming access code, default is 99. Bin 96 holds the accounting access code. Default is, you guessed it, 96. You would be surprised to know how many phones are still in default. Ain't it wonderful? Using the ANI number supplied by *2600* will yield any COCOT number that is not on the outside of the phone. Call the phone and enter 99. If you gain access, it's fun to play around. ##0 will reset all bins to default (except

password, time, and date). ##10 will reset the rate table bins to 0. ##11 will enter the rate table adjustment mode. Bin 11 is the rate for local calls and Bin 12 controls the Intra-Lata (1+ seven digits) calls. Bin 14 controls the long distance calls. Naturally, I can never go back to the phone's physical location and open it. But it sure is fun to call it. Less than thirty days after I did this the phone was replaced. Guess what? The lock mechanisms had the serial numbers stamped on them!

Mr. T.

Suggestions

Dear 2600:

In your last issue you had an article on building a telephone coil which I thought was irrelevant as far as the recording of the red box tones. There is a simpler way of doing this which has worked better. Radio Shack sells something known as a Telephone Pick-up which goes for about $1.99. This plugs in straight to the "mic" of the tape. Obviously, one has to then go to two adjacent phones and do their deed. However, instead of looking for two adjacent pay phones, you can have your mother/father/ brother/ sister/ friend/dog/rat etc. go down to the pay phone and deposit the quarters for you while you stay home and record them on a tape recorder. From experience I suggest using a metal tape for longer duration. Secondly, don't leave this tape in the car or the sun since it may change the pitch of the tones and ACTS will have a hard time picking it up and thus you will be considered a failure.

I enjoyed the tone dialer conversion article tremendously and thought it was a great idea. Keep up the good work.

What I think *2600* should do now is introduce new BBS's. When Central Office and Toll Center were running it was great! The communication between hackers is very important. The next generation of hackers will soon be there to take over and all they will be interested in is "codez". These days the BBS's in the hacker community are generally filled with "codez-asking" kids. No real knowledge is passed on. The Toll Center had rooms to introduce new ones to hacking which was fantastic. Both your bulletin boards networked, which was wonderful. Now the BBS world lacks such boards to call. Think about it.

The Concerned!

We are.

Technical Suggestions

Dear 2600:

Just picked up a copy of your zine at Dark Carnival in Berkeley. Keep up the good work. Some comments on "Hunting for Wiretaps" (Summer 1990, page 24):

Telco does not use series wiretaps, nor does Sprint. The analog hybrid line going into your telephone goes into a SLIC (Subscriber Line Interface Circuit) in the exchange, where a chip called a CODEC (coder/decoder) converts it into a digital PCM (pulse code modulated) stream. This is what actually gets switched in those 5ESS switches Bell likes to talk about. If you are Bell or the NSA, it is a simple matter to order the switch to send you a copy of someone else's bitstream. This is a wiretap in software, for all practical purposes impossible to detect.

Fortunately, most FBI agents know less about the phone system than a dead mule and are equally immune to advice. Twelve volts sounds about right for the analog line while conducting a conversation, but it's more like 100-150V to operate the bell. The lines have a high voltage rating, about 300-500V before the telco surge suppressors cut in and twice that before the SLIC starts to burn. Op amps, on the other hand, have a maximum rating of a hundred volts or so, which is why some lines behave funny when they are tapped (fails to ring or fails to answer when picked up, or very poor audio quality).

The best way to test for an op-amp would be to discharge a photoflash capacitor (330 UFD at 300 volts) into the line and look for the bright flash of light as the op amp went to that great transistor in the sky. But use some caution, as the capacitor is *not* a toy. Get a friendly telco person to unplug the SLIC and tape down the ends of the line with dielectric tape and do the same with your end. Confirm that there is no lineman working on the line or on a nearby one. Then double check. The capacitor is easily capable of killing a human being as well as a fifty cent IC. Don't connect a 300V power supply directly to the phone lines or you are likely to hurt someone - probably yourself. Bleed the voltage off both the capacitor and the line before untaping anything. If you can't

get a telco person to help you out, drop the project. This method is safer than dangling from telephone poles poking at high voltage lines with a multitester, but it is still very easy to fry someone.

As for downing a 747 with a phone call ("Plane Crash", page 31), a lot of the early portable computers were very lax about FCC guidelines for emitted RFI. Think about putting a mobile phone inside an early Compaq or Kaypro and handing it to a passenger as carry-on luggage. Then dial up the box while it's in the air and download a few files. The electromagnetic garbage emitted by the PC could jam the 747 "fly by wire" avionics, leaving the pilots with no control over the plane. If you want a collision, do the deed during takeoff or landing - the 747 will be more likely to hit something. It should be fairly easy for a hacker with a scanner to intercept the fatal call, although identifying the guilty party might be more difficult. Perhaps your hacker can read the packet headers and trace the call? Or his girlfriend is a cop and she traces it for him?

AP
Oakland, CA

Caller ID Override

Dear 2600:

From what you know about the caller ID systems that are gradually being introduced, do you think it would be possible to build a circuit or add-on box to your own home phone to send a false number to the party you are calling? It would seem to be the ultimate defense against the invasion of privacy while at the same time giving the appearance of cooperation without a "P" for privacy showing up on everyone's caller ID screen.

Pete
Akron, OH

Absolutely. We hope to see someone do this soon.

A Phone Company Tour

Dear 2600:

I had the opportunity recently to tour the 4ESS owned by AT&T here in Cincinnati. I went along with a tour offered by the local chapter of the American Society of Mechanical Engineers. It was an interesting office, because four or five different levels of technology were present in the same building. These ranged from hardwired, dedicated lines leased by companies and corporations for direct data or voice communication between distant locations (Saks Fifth Avenue can pick up a phone here in Cincinnati and immediately ring a phone in the New York office without actually making a long distance call). I gathered that this was a pretty expensive option and would only pay off if you made a hell of a lot of calls to the same long distance point. This system was still using the old style plug-and-socket boards that were the rage earlier this century.

There were no mechanical switches in use, but there were several levels of electronic switching ranging from large, outdated analog circuit boards to the new fiber optic system that they were still in the process of installing. The whole system was backed up by a roomful of massive wet cell batteries that would supposedly keep everything humming smoothly for about eight hours after a power failure.

I was surprised to find that there are only 15,000 outgoing long distance lines emanating from the Cincinnati 4ESS. I had suspected that there were many times that number since this is such a big area with so many customers. I was also amazed at how small the cable cluster coming into the 4ESS from the Cincinnati area central offices was. I would estimate it to be only a couple of feet in diameter and it was entirely unprotected once it entered the building. (I hope no terrorists are reading this.)

The AT&T fellows were quite knowledgeable and informative. They even attempted to go into a little switching theory; obviously thinking that a group of mechanical engineers would be appreciative of such information. I was, but my fellow engineers were busy asking questions like, "Is there really a single wire that runs from here to California that you talk over?" and other questions similarly asinine and inane. I was embarrassed for them and hid my head in shame.

I totally struck out in asking questions about the ANI for this area, and in wondering aloud why the phone company charges for touch tone service when the whole bloody system is based on those magical little tones. I, of course, scanned all visible paper for phun numbers, but everything was well hidden. My mouth

watered when I saw the full set of operational manuals for the 4ESS sitting out in the open.

A major alarm went off in the system while we were listening to switching theory. It seems that someone dug into a large and rather important cable cluster somewhere in eastern Cincinnati, thereby cutting three or four central offices off line for a while. The technicians on duty knew what had happened in about fifteen seconds after the printers started dumping trouble codes. One of the guys even let us peer over his shoulder as he accessed one of the downed connections and did some diagnostic checks. Pretty neat, that.

Well, enough about my little tour. Now to some suggestions for future issues: program listings for an IBM compatible computer for a blue box, a red box, and some dialing programs (modem searches, extender searches, etc.); comprehensive listings of exchanges other than New York area; ANI and CNA (with access numbers) for the 513 area code; more BBS numbers; book reviews; equipment reviews (scanners, pen registers, phones, computers, and other things that can be used for hacking and phreaking); more hands-on information; and information on ATM machines and their ilk.

Mitch
Cincinnati

Assorted Thoughts

Dear 2600:

In my area, Ma Bell finally improved one of their long abused holes: they got rid of the operator for collect calls. One can no longer bill to another number or make a collect call with a human operator. Instead the system will ask for your name and digitize it and play it to the destination to verify the billing. So the person you're billing will probably recognize whether or not the person is actually who s/he claims to be. It sure took them a while to figure that out.

Anyhow, with this procedure one can also make five cent local calls from public pay phones. The good part is that it's completely legal. Just bill the destination and when the system asks for a name, say the phone number of the pay phone. Hopefully the person who picks up on the other end has some common sense and calls you back. So now you don't have to carry around any change and you still save yourself a good twenty cents (it does add up eventually!).

By the way, Sprintnet (also known as Telenet) is doing some sort of deal with transmitting data in printed form to addresses via US mail. Does anyone happen to know how to access it? I'm using it through a net but it's too expensive. I'm pretty sure there's a way to do it directly.

Keyboard Jockey

Call 800-TELENET and ask them about that service. MCI Mail has something similar if not identical. You can always use an operator for collect or third party calls if you don't have a touch tone phone or if you say you don't.

Dear 2600:

I really don't want to write another one of those "Gee, I really really like your magazine...." letters, but unfortunately that is exactly how I feel. I am in my mid twenties and way, way back in the silicon dark ages (put it this way, I can remember when the IBM PC was thought by some to be a flash in the pan that would never oust the Apple II as the market leader) I discovered computers and modems. I had a second-hand Apple II+ (which I still use with pride and some choice hardware enhancements), a Hayes Micromodem II (since upgraded to a Practical Peripherals 2400 external), some "borrowed" software and a lot of naive curiosity. I was never a "hacker" per se, since I have about a third grade computer literacy level and the extent of my hardware knowledge is knowing what card plugs in where, and I did do some things in that dark time right after the breakup of the phone company that some water under the conscience tells me were not too nice, but I really didn't know any better.

With my little toy I discovered a whole new method of communications, with the immediacy of a telephone call and the depth of a letter to the editor. It also opened up the world of everyday technology: I heard about the rainbow of boxes that certain people use to test the limits of the phone system that 99.9 percent of people (myself sometimes included) take for granted. I heard about different computer systems and how to get into them. Frankly, I've never really wanted to hack myself, but it's always been fun to find out how I could do it, and stories from those who did such things were always fun to read.

In short, I experienced what the framers

LAST OF THE LETTERS

of the U.S. Constitution had hoped for when they sat down in Philadelphia in 1787: the free and open exchange of ideas (to borrow from WABC's Bob Grant). Even if the information shaded a little to the gray, it was still useful. But, freedom and paranoia go hand in hand: if you are free to do what you wish, eventually the exercise of that freedom may impinge upon the freedom of someone else. That is why we have laws, some fair, some not. Now, I'm not saying that laws cause criminals because there is a certain percentage of humans who will always do things at the expense of other humans, but I do believe that unfair laws will awaken otherwise latent tendencies in people. Since people will increase their "law-breaking" in the face of unfairness, those in power will retaliate with tougher laws, and so it spirals up until it can go no higher and suffocates in the stratosphere of social collapse.

What does this have to do with *2600*? Your publication is one way responsible citizens have of combating the unfairness in our post-industrial society. Since information has become power in our society (witness the inordinate influence that CNN has over government policy), those in power, whether they are government or business, find it incumbent upon themselves to control what people know. Fortunately, we live in a more-or-less free society and we can get access to information *if we dig for it*. There is enough self-incriminating information spread across all of the U.S. government's own pamphlets and press releases to keep self-appointed "government watchdog groups" in Brooks Brothers suits, but that information is not publicized. So maybe the key to our so-called "Information Economy" is publicity. Sure, IBM gets all the publicity for marketing a bug-ridden, hard-to-use computer, and Apple Computer can "Win the Hearts and Minds" of computer users, but who outside of semi-hardcore computer buffs know about the Amiga, or even Steve Jobs' neXT? They can blow the disk drive doors off even a fully-loaded IBM power user's dream machine, but who's really heard of them?

So this isn't the "Information Age", it's the "Publicity Age". As Adolf Hitler said, if you must lie, tell the most outrageous lie you can. It's easier to believe that way.

The Disco Strangler
South River, NJ

COCOT Info

Dear 2600:

Thought you'd be interested in the following. I called the COCOT you listed (212-268-7538) and noted it answered with a computer tone and an ASCII blip. Upon recording this blip and playing it through a computer modem, the following was generated:

T:@*2122687538*33725*CA2107*8934*087*9012216073424*00000-

Attempts to hack into the COCOT resulted in being disconnected. I could not get any kind of response other than the above at initial connect. This was done at 300 baud.

Waterbury, CT

Dear 2600:

This is just a little something interesting we've discovered. The phone numbers (both in the 212 area code) are the ones which appeared as a response to a letter about the article on COCOT's which appeared on page 31, Autumn '90. The two numbers connect at 300 baud and send the following alpha-numeric strings.

212-268-6129:
T:@*2122686129*41465*CA2202*6837*142*9101116171141*00000E

212-268-6129:
T:@*2122686129*41465*CA2202*6837*142*9101116171205*00000D

212-268-6129:
T:@*2122686129*41465*CA2202*6837*142*9101116171228*00000?

212-268-7538:
T:@*2122687538*51880*CA2202*7637*222*9101116171435*00000

The Martyr and
The Mute & Bach Wai

Now this is what we like to see. Readers taking it upon themselves to go further with the information we print. Is there someone who can explain what these numbers mean?

2600 is always in need of writers! If you've got a field of expertise or a story to tell, send it in to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953
Questions?
Call (516) 751-2600

CAN YOU BELIEVE THE THINGS PEOPLE SEND US?

OUR CONTEST

In our Summer 1990 issue we published a bunch of negative letters that were written about hackers. We invited our readers to come up with replies. The winner would get a free lifetime subscription. We got a pile of really good entries. And when the dust cleared, we realized that we had two winners. Unfortunately, neither of our winners did a very good job of identifying themselves. So we have absolutely no idea where to send the subscriptions. If you recognize your piece below, contact us and think of some way to validate your identity.

Entry Number One
by TELEgodzilla

I found the Summer 1990 issue very intriguing - particularly the section dealing with the other point of view against those who attempt to learn more about systems. As I was reading these letters of anger, shame, and disgust, I was struck by how similar this situation is to what Dr. Richard Feynmann experienced during the development of the first atomic bomb.

In the book, Surely You're Joking Mr. Feynmann, there is a chapter relating how Dr. Feynmann was able to crack open U.S. Army safes which held the plans and makings of the then being developed atomic bomb in Los Alamos (chapter entitled "Safecracker Meets Safecracker", pages 119 to 137, Bantam Books). Feynmann had discovered, after speaking with a safecracker, how most safe factories give a standard assigned combination number to safes, instructing the buyer to reset the locks. Most buyers, however, didn't bother reassigning their safes with new combinations, failing to realize that the standard assigned number was just that - a standard assigned number for *all* safes then being made. What Feynmann did was go around and open the Army's safes within the Los Alamos compound (he was able to open one out of every five) with little trouble for nobody had thought of bothering to change the combinations after the safes arrived from the factory!

How was Feynmann treated? With respect and understanding? On the contrary - he was nearly thrown out! Did the Army change the safe combinations? Sure - eventually, but not until after several months into the project.

So you ask yourself - what the hell was Feynmann doing? Couldn't he just leave well enough alone?

No; Feynmann had a curiosity - the very same curiosity which led him to develop new and better understandings of the atomic sub-structure led him also to find ways in which to open up Army safes.

This is the crux of the argument and controversy surrounding hackers: people are naturally curious. Trying to stop this curiosity from enveloping the world around us is akin to trying to stop a mountain of water. Even if we did, it'd only bring about more trouble (besides developing new and wild forms of nervous neurosis), for man is differentiated from animals on many points - and chief among these points, curiosity rules the pack.

It's fascinating, but none of these letters spoke of harnessing the very same curiosity and drive toward protecting their systems. Instead, we all merrily throw things about, rant and rave about how terrible it is for people to go "walking through their house" without stopping and considering how to find out ways of positively utilizing the skills and powers of those capable of doing so.

But an even more important point not being raised throughout any of these discussions is the fact that perhaps privacy is nearly dead - and it ain't by those "kids".

When you stop and consider how many files the U.S. government has on each person - whether you're in the armed forces, receiving or have received a college loan, possess a driver's license, hold a social security card, maintain a farm or a grocery store, pay taxes on a regular basis, etc. - the fact of the matter is that there are bigger and more nasty people who rummage through your house on a regular

WINNERS

basis - and *you don't even realize it!*

Protection of our credit records is probably one of the greatest non-issues today. TRW or Dunn and Bradstreet regularly sell information on your credit status and income standing to corporations which seek only to find new markets to sell their products. *It's a point of rule that every time you receive junk mail, somebody accessed your credit records.*

And we're worried about punk kids taking a walk through telephone companies to get information that they could receive by the mail for $13 - as the Neidorf case proved?

Somehow the real criminals are getting away scot-free.

I respect people who take the time and effort to find ways into computer systems, for we all learn much from it; it keeps us on our toes. And in this apathetic society I also feel better when I know that there are people who *do* care about the world around themselves and take the time and risks upon themselves to learn more.

That's not only curiosity, that's entrepreneurship. Equality is never something given; it is only achieved and maintained through diligence and persistence. Having information hidden away is anathema to democratic freedoms. Seeking out information makes us grow and become more competitive on the world market; this is what makes our country great.

As a professional operative, I think many of these people would be mildly shocked if they found out to what extent and degree private and public institutions employ people such as myself, and how much information is constantly available on the average citizen.

I have little regard for those who brand "hackers" as threats for no other reason than for their impassioned curiosity. Grow up yourself! This is a bigger world than you realize and, as a professional, I frankly find this talk of anger to be utterly misdirected and somewhat naive. Attack TRW, Exxon, the Republican Party.... Any corporation - public or private - possessing of multi-faceted interests is inevitably going to have some sort of computer system and with that system are those who are going to make sure that it works - even if that system is meant to take information about your checking account, car insurance payments, psychiatric care, or even if you had recently purchased any Elvis records!

It is not surprising that the majority of these hackers are young. We should come (and pray) to expect more of these individuals to arrive into prominence, for we are a country that is losing touch with its people, most particularly its youth. Here we stand, bitterly complaining how many youths cannot read a map (much less actually read) and yet we have those able to discover new means of accessing information which even the so-called "experts" never realized existed!

We are punishing talent that this country desperately needs, rather than reaching out to exhort this raw and excellent energy into new and vital means beneficial to all - particularly those who possess this great inner strength.

No, don't go for the kids who rummage through your garbage; go for the faceless professional bastards who keep and maintain a detailed profile on you so that they can sell you watches, cars, beer, and, yes, political issues. For it is they - those who maintain those giant mainframes without even *bothering* to think about the consequences (as well as those who rule) that we should be watching.

The child who discovers that the emperor is nude should never be punished. It's time that we start noticing these little details.

Entry Number Two

I'm a hacker. I worship the computer and the endless possibilities it poses. I see programming as an art, and I was born to explore. When I sit down at my computer to do something, I don't debate in my mind whether or not what I'm doing is illegal or

unethical. I just do it. The computer is a medium which is so immediately explorable, with a scope so infinite and a depth so limitless that it makes "just doing it" extremely feasible. That being the case, there is more to a computer than programming, and those with an insatiable instinct to learn and know easily assimilate themselves into the abundantly different aspects of the computer world and, inevitably, into aspects associated with underground activity. This type of person, the hacker, does not think in terms of right or wrong, as the definition of these terms depends on how you look at life in general. The means is the ends, and the ends justify the means. Columbus was a hacker. He explored new worlds because they were there. He didn't stop to wonder what effect his discovering the New World would have on the Native Americans. He just did it. Leonardo daVincci was a hacker. He explored the human body, among other things. In his time, it was forbidden by the church to dissect dead bodies to find out what made a human tick, but he couldn't care less what the church had to say about it. He had a desire to know, so he just did it. Humanity has a history of wanting to know and this desire to know sometimes leads to questionable means. Questionable, depending on how you look at it. If it wasn't for the hackers of different sorts throughout history, where would humanity be now? Although we probably wouldn't still be dressed in animal skins if people had always remained complacent to those in authority and shied away from those things that we "weren't supposed to do", we wouldn't be as nearly advanced a civilization as we are today. It's because of those people who dared to know and had the desire to understand the world around them that we are at the point in history we are today. We owe a lot to hackers.

Although I'm not a gung-ho systems hacker, I've done enough to understand the thrill and relish the challenge. I was once under surveillance by the phone company for "being where I shouldn't have been," so I feel I'm at least that much more qualified to comment on this subject than your average Joe computer user. It's called experience, and that's something I have a fair amount of due to that peculiar instinct we all have inside of us called "hacking".

Some people believe that when you hack you are going somewhere you do not belong and equate this to breaking into someone's home. This is a stupid analogy that is much overused. Hacking is a game as much as life is a game. If you choose to play, you accept the risks associated with it. If you win, you win, and if you lose, you lose. What are the rules? What are YOUR rules? You play the game as you wish and you deal with the consequences as they come, and only your conscience and personal integrity dictate where the game leads.

Scenario: You break into a house and you start looking around for something interesting that will tell you about the owner. Many things can happen at this point, one thing being the owner of the house wakes up and finds you rummaging through his file cabinet, whereupon he pulls out a .357 magnum and blows a two-inch hole through your chest and you die.

You can see how the analogy between hacking into a system and breaking into someone's house doesn't hold up too well when you really put any thought into it. When someone goes through the trouble of breaking into a home it is usually for malicious intent (i.e., to burglarize, rape, etc.) and rarely just to dig through personal files (which is not the definition of hacking anyhow). Hacking is something you do casually in the comfort of your own home. With the majority of hackers, there is little likelihood of any intent to do harm, but rather an innate curiosity. Can the same be said of a burglar or a rapist walking into an unlocked home? Someone breaking into a residence usually has premeditated a crime. A hacker is merely exploring. If, in the process of exploring, a very tempting bit

OF THE HACKERS

of information is found, the hacker must make a decision: does he download the file or leave it be? If you go to buy a newspaper from a machine and find that the last person to purchase a copy left the door open, do you take a copy without paying for it? Nobody would probably ever know if you did or not, so the question comes down to your personal ethics. Do you take it or leave it? What are your rules?

Scenario: This strange system you've just hacked into turns out to belong to one of those mailing list companies that sells your personal information to those annoying sweepstakes and mail order firms. Is it alright for them to sell your personal information and for you to be looking around in their files? Is it wrong for them to be selling your personal information as well as for you to be looking around in their files? Neither? Either? Both? What are your rules? They're making money, which they enjoy, and you're learning the system, which you enjoy. Are they wrong for wanting to make money? Are you wrong for wanting to learn? What are your rules?

Now let's say you've done something particularly heinous, such as broken into a Bell South computer system and heisted some file called something like "E911 Overview" which is purported to be worth around $79,449 (actually, $13 with a $79,436 legal fee). Eventually the all-powerful and all-knowing Secret Service, that institution of unfathomable intelligence, tracks you down and decides to smite thee and all in your path with its mighty wrath. Well, now you've been caught. You played the game and landed on "Go To Jail", and you ain't passing go, baby. You took the risks and lost...but the game is more complicated than that.

Since we all have to participate in this game whether we like it or not, it is necessary to explore the effects of this broad-scoped action taken by the very government institution which we entrust to protect our God-given rights. The minute details cannot be ignored, as they are the scariest and speak the loudest in terms of criminality and injustice. Yes, even more so than that evil 19-year-old punk with the ego.

This treasure dubbed the "E911 document" makes its way through numerous systems via a network, unbeknownst to the owner of each particular system. The SS (Storm Troopers), while tracing this document's trail, come across one system that the document made its way through. To them, it's obvious that this system was involved in this plot to disable the emergency phone system and lead to the downfall of the government, the country, the world, and then eventually life itself. So they see no problem with confiscating this system and everything else that looks suspicious inside the abode where it dwells: the disks, notes, books, magazines, music tapes, stereo, TV, lamp. No, not even the toaster is immune from this rampage. Hey, it's got a cord on it; it *must* be involved in this devious scheme somehow! Maybe the person being stripped of all his possessions and dignity at this moment, who in all likelihood is being physically restrained by four men in dark sunglasses, his poor mother in handcuffs with a double-barrelled shotgun pointed at her head (she just *might* try something, you know) is some undiscovered super-genius who has developed a method of encoding data on toast. They want to check those bread crumbs at the bottom just in case.

Scenario: Someone who has just burglarized a home runs through your yard as he attempts his getaway. The cops trace his trail through your yard. Are you now guilty by association? Do the cops rampage into your house with destructive force, confiscate all your possessions and terrorize you and your family members to gather evidence that proves that your neighbor's house had been burglarized? No. Is this analogy more suitable than the one so commonly overused by those who

(continued on page 46)

We've published information in the past on AT&T's USA Direct. Out of fairness, we should tell you that there are other similar services that allow you to call back to the United States from other countries without having to deal with local operators who often don't have the common decency to speak our language. You can now avoid foreigners on the phone by using Sprint Express. You'll be connected with a Sprint operator in the United States who won't disrespect you. Some countries and the numbers to call from them: Argentina: 001-800-777-1111; Australia: 0014-881-877; Chile: 00, wait for tone, 0317; Colombia: 980-13-0010; Denmark: 8001-0877; France: 19, wait for tone, 0087; Hong Kong: 008-1877; The Netherlands: 06, wait for tone, 0229119; Japan: 0039-131; Singapore: 800-0877; United Kingdom: 0800-89-0877. All of these connections are toll-free. You can bill calls to a FON card, call collect, or use your local calling card.

***

There's also a new Sprint service that allows you to conference calls. It only works on FON card calls and not on 10333+ or 950-1033 calls. When connected to a call, hitting a star for a full second will put you in conference mode. You can then dial 12 which puts the first call on hold. Then you dial the area code and number of the second call. After the second call answers, you hit another star for a full second, then dial 13. The second call is now linked to the first. If you want to disconnect the second call without linking it, dial 14 instead of 13. There's a 75 cent surcharge on top of the regular FON card surcharge (times two) on top of the charge for the two phone calls. Maybe someday they'll finally get it right.

***

Allnet has a whole host of services they've been introducing. By calling 800-783-1444, you can place calls by dialing 0 plus the number followed by your Allnet calling card number. Or you can dial a two-digit "Speedlink" code followed by a star and then your calling card number. This will connect you to a variety of airlines, hotels, and car rental establishments, all of which have toll-free numbers already, so you'd have to be kind of crazy to spend 20 cents a minute using *this* service. If you hit a star after connecting to Allnet's 800 number, then enter your calling card number, you'll be able to access InfoReach (recorded announcements on the stock market, horoscopes, sports, entertainment, and international time and weather costing between 30 cents and 70 cents a minute), Call Delivery (for $1.60 you can record a brief message for immediate or future delivery to any phone number in the U.S.), Voice Mail (with a 7-digit ID number and a rate of 38 cents a minute), and Teleconferencing ($2.00 for the first minute, 49 cents a minute for each caller). In its little brochure, Allnet urges its customers to "power dial" and save. What does this mean? It's rather frightening, actually. It seems that Allnet now charges calls from the moment you access the Allnet dial tone. (They swear they won't charge you for uncompleted calls.) Allnet says, "Don't wait to hear every word of a prompt or the end of a tone before you continue dialing. If you know the next step, start dialing as soon as you hear the beginning of a prompt or tone. It saves time, plus you won't be charged for time spent listening to instructions you don't need." This is the first case we're aware of where a long distance company blatantly admits charging its customers for the time they spend *dialing* the call.

***

Allnet also has an international call-back service like USA Direct and Sprint Express. They call theirs Option USA. The countries and numbers are: Australia: 0014-800-125-197; Belgium: 118671; Denmark: 8001-0658; France: 05-90-2919; Greece: 00800-12-2100; Hong Kong: 800-6159; Israel: 00177-150-1067; Italy: 1678-97038; Japan: 0031-12-2453; The Netherlands: 06-0228491; Spain: 900-99-1450; Sweden: 020-79-3934;

Switzerland: 046-05-8812; and United Kingdom: 0800-89-2695. Canadians can access Allnet by dialing 800-955-1444.

***

With all the fussing and fighting in this country over Caller ID, it's interesting to note that British Telecom *refuses* to provide the service. While privacy may still hold some appeal over there, so do rip-offs. Several companies have sprung up offering CLI (Caller Line Identification) devices even though it's technically impossible since British Telecom doesn't pass along the number of the calling party. So how do these companies manage to make these offers? Their devices simply ask the caller to enter his/her phone number before the call is completed. Lo and behold, the number that the person entered is displayed on the called party's magical device as soon as the phone rings. And the person can enter any number their heart desires. In other words, this is about as far from Caller ID as one can get.

***

According to an internal NYNEX memo, the systems known as COSMOS (provisioning) and TIRKS (trunk assignment) will be replaced by the new Bellcore-designed system known as SWITCH. "It's time to take advantage of the advances made in computing technology" over the past 20 years, say the people in charge. SWITCH, which stands for absolutely nothing, is scheduled to be installed in late 1991, with implementation to follow a year later. The new system is actually divided into two parts: SWITCH is the "provisioning" part of COSMOS and will require synchronous terminal access, whereas FOMS, the frame work management part of COSMOS will require asynchronous terminal access. All current COSMOS users in NYNEX and its children (New England Telephone and New York Telephone) will be getting a "network terminal survey" to evaluate the needs of the future. SWITCH was first mentioned in *2600* a while back but it now seems close to reality. We imagine similar plans are being made all around the country.

***

According to the Amsterdam (NY) police department, a former resident "known for causing mayhem with telephone and computer lines" has been connecting their phone lines to people all over the world and billing it back to the police. "We pick up the phone and we've got the Los Angeles sheriff's department on the other end," they say. Newspaper reports claim the villain is able to gain access to the "telephone computer system and use the police department's access code". The translation of this is that he/she is able to get and use a calling card number. According to a friend of this nasty person who contacted *2600*, the police have "harassed my buddy for years. Now there's a war between [this person] and the police...for over two years. My friend is a notorious hacker."

***

If you're a gang member in Los Angeles, you may get to take part in an exciting new technology experiment. Whenever there's a hint of trouble in the area (gang wars, retaliatory strikes, etc.), known gang members who are also on probation will be placed under electronic house arrest. These subjects will have created a "personalized template" by repeating the names of 22 states three times in succession to a computer. The computer will then call the gang member at a random time and ask him to repeat eight states. If he doesn't pass, it will call back to give him a second chance. If he fails again, the computer calls the probation officer's beeper. And a recording is made of the failed response. Our question is this: don't most gang fights take place late at night? If a gang member has to stay home instead, maybe he'll want to go to sleep at a normal hour. But how can he when he's going to get a phone call from a computer? Also, what happens if the phone is busy? Is using the phone going to be illegal during house arrest? Will call-waiting become mandatory? And what if the gang member is using a modem? Will call-forwarding be

illegal? And what happens when a clever gang member invents a voice recognition system that is able to generate a response in his voice when it hears the name of a state?

***

Hi tech is also coming to the rescue of police/informant relations. By dialing into a computer system called CASSIE SX-4, informants can leave messages for their police contacts. CASSIE will then page the police officer. Ross Distributing of Upland, CA claims the system will provide more security because "only the officer knows his password". For $4000 you can get software that can handle up to 75 mailboxes. You'll still need an AT compatible computer. For around $15 a month you can get a single line voice mailbox through the Yellow Pages that does basically the same thing.

***

The next time you get all frustrated at a payphone, think of this: the cost of a local call at a payphone in Poland was recently raised to 20 zlotys (still less than one American cent). But 20 zloty coins have become a scarce commodity since they're in such demand. There are two other sizes of 20 zloty coins that can be found quite easily. But they don't fit into the phones. There's also a 20 zloty bill but that doesn't fit into the phone either. So what do people do? What else is there to do in Eastern Europe but make use of the black market! There you'll find all the 20 zloty coins you need — at a cost of between 200 and 1000 zlotys apiece.

***

Illinois Bell is applying for Caller ID. The following excerpts come from the December 1990 issue of Illinois Bell's Telebriefs newsletter: "Illinois Bell believes that a person who receives a phone call is entitled to the same information as the person who makes the call, namely the phone number of the person at the other end of the line....Illinois Bell is proposing to offer Caller ID without the blocking feature that some groups have proposed. With the blocking capability, abusive callers would be able to prevent their numbers from being displayed, thus diluting the benefits of Caller ID.... When it is necessary for individuals to maintain their anonymity, operator assistance, calling cards, public phones, and cellular phones can be used." What they don't seem to be taking into account is the fact that abusive callers can take those very same steps to maintain their anonymity. Since it's technically impossible to identify someone who uses the above methods, very few abusive callers will continue to dial direct. Which leads us to believe that, despite their sales pitch, Illinois Bell is really interested in Caller ID'ing all of the non-abusive calls. Of course, if they phrased it that way, people might just think twice.

***

New Jersey Bell has really pulled one over on the public. Remember when 900 numbers first started being dialed en masse? New Jersey Bell, and most other local phone companies, told us not to worry; it was easy to block such calls and it didn't cost anything. Now if you want the privilege of not being ripped off by 900 and/or 700 numbers you have to pay a one-time fee of $5. Then there's another one-time fee of $16 to process the order! Businesses have to pay even more. In all likelihood, less than ten keystrokes are required for the whole order. It's bad enough to see so much cheating going on in the phone business, but ripping you off to protect you from being ripped off is more than most people deserve.

***

Some British statistics: More than 99 percent of the 80 million calls made every day get through on the first try; about 90 percent of calls to "directory enquiries" get through on the first try and seven out of eight of those are answered within 15 seconds; ninety-six percent of British Telecom's 95,000 public telephones are in full working order at any one time; and, on the average, a "fault on a line" will occur only once every six years.

our exciting world

According to British Telecom, "Nearly 11 million customers are now connected to local digital exchanges. And more than 70 percent of customers are served by modern digital or electronic exchanges offering faster connections, clearer lines, and fewer call failures.... Unfortunately there are cases where we fall short of the high standards we set ourselves. To put things in perspective, even if we fully satisfy 99.9 percent of our 25 million customers, we will still have 25,000 who are disappointed."

***

The British have also done away with an unfair charge that we in the States still contend with. There are no longer connection charges for customers who take over an existing telephone line without a break in service. In other words, if you move into a house with a phone line already installed, you won't have to pay for the phone company to switch the account to your name.

***

A couple of other British tidbits from phone company publications: "Push-button phobia is stopping millions of people getting the most from their telephones. Almost half of British Telecom customers have digitally-connected homes, but few know, or try to find out, how to take advantage of all the phone's functions. For example, the cost of BT's operator-alarm service has doubled from 1.20 pounds to 2.47 pounds but for just 13p a call you can programme your phone to wake you up. Simply pick up the receiver and dial 'star 55 star' followed by the time you want, using the buttons on the phone's tone pad for hours and minutes. To check you've got it right press 'star gate 55 gate' and the exchange's synthesised voice gives the alarm time. To cancel the alarm call simply press 'gate 55 gate'." But all is not well in the U.K. This letter recently appeared in The Sun: "British Telecom services have improved immeasurably since it cast off the shackles of State ownership. We may not like the new telephone boxes, but at least they work. The company still gets complaints, but at least it responds to them. So we hope it will reconsider plans to charge 35p for Directory Enquiries. BT is now ringing up profits at the rate of 8 million pounds *a day*. It has a duty to shareholders, but must not forget that although it is a private company it is still supposed to be a private service."

***

About the most useless thing we've seen in a very long time is the AT&T Callers' Club. It came in the mail a couple of months ago demanding attention. "You've already earned your membership just by being a great customer. There's nothing more you need to do, and no strings attached." There also seems to be virtually nothing this "club" has to offer. There are promises of "previews and discounts for new AT&T products" like Voicemark, AT&T's messaging service that we wrote about last issue. We doubt AT&T won't tell "non-members" about their new services and so far we have yet to see any discounts that couldn't be obtained in the real world. We're also privy to announcements of "AT&T sponsored events" in our area. Wow. Unless that includes hacker raids, we're not impressed. A chance to win "fabulous prizes" and "valuable savings". Again, nothing we haven't heard before numerous times. Finally, a toll-free number reserved for "members only" (800-223-2000). We can use this exclusive number to "find out about discount periods and calling plans, receive immediate credit for misdialed calls, ask about your bill, get prices for the cost of a call between specific locations, order your AT&T card, learn how to access AT&T when you're away from home, and notify AT&T when you move, so that you can continue to receive your Callers' Club benefits without interruption." We are flabbergasted. There is *nothing* here that you can't already get by dialing customer service (800-222-0300) or your AT&T operator. We don't know what AT&T is up to with this gimmick but we'll keep everyone informed. By the way, they sent everyone a

(continued on page 44)

To Our New York Telephone Customers

Beware of Telephone Fraud!

Recently some unscrupulous people—posing as security officers from New York Telephone or other telephone companies, or identifying themselves as federal or police investigators—have tried to deceive and cheat New York Telephone customers. With the excuse of helping them in their "investigations," these "agents" ask you to accept the charges for phone calls from people that you don't know and in some instances they even threaten law suits or suspension of your phone service if you "don't cooperate."

Please, DON'T FALL INTO THIS TRAP. Don't let strangers charge calls to your phone number. New York Telephone is **not** asking for its customers' help in catching crooks.

DON'T BE FOOLED by these impostors that have nothing to do with New York Telephone. If you have questions or doubts, call your New York Telephone Business Office at the number that appears on the first page of your telephone bill. We're here to help.

We're all connected.

New York Telephone

A NYNEX Company

WE DON'T KNOW WHAT'S GOING ON, BUT RECENTLY EVERY CUSTOMER OF NEW YORK TELEPHONE GOT THIS NOTICE.

2600 Marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011,212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

RESEARCHER/WRITER seeking inside information on credit bureaus for story on privacy issues. Please call 301-702-1009 after 6 pm, ask for Edward or write: 3311 Dallas Drive, Temple Hills, MD 20748.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

FALCON would like to trade knowledge and codes with other hackers. Also interested in trading the latest videos, music, etc. Falcon, PO Box 1038, 7550 BA, Hengelo, The Netherlands.

CONTROVERSIAL DTMF DECODER as shown in the Spring 1990 issue. Exclusive offer to 2600 readers: complete revised plans with layout and explicit instructions for construction. Information and hardware commercially sold for $$$. Sending a SASE (with .75 postage) nets you 9 pages of data for the stamp!!! Decoder chip and PC board available. W.E.B., PO Box 2771-H, Spring Valley, CA 91979.

ANTI-WIRETAPPING bug detection, privacy protection, information services, new and used equipment. State of the art equipment beyond today's technology! National computer search system, information research service. Retail/wholesale, surveillance and countermeasures equipment. Call E.C.I. Free consultation hotline: (516) 929-3261.

LOOKING FOR SOMEONE to correspond with to get a basic understanding of hacking and phreaking. (I am in prison.) As I would like to ask questions, please write me directly. If you wish to use a nickname that's fine. Just make sure you write it as your return address or it won't get to me. Victor Mendoza, 9601 NE 24th St. 410216, Amarillo, TX 79107-9601.

OLD TAPES of telephone recordings, rings, busys, etc. wanted for radio programs. Also, current recordings and funny phone calls welcome. Send to Emmanuel, PO Box 99, Middle Island, NY 11953.

WANTED: Red and blue box plans/kits and assembled kits. Also, expansion cards for a 256K Compaq. Please contact Charles Silliman, 11819 Fawnview, Houston, TX 77070.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

WANTED: Atari ST hacking/telecom programs to trade. I have Mickey Dialer and 2 tone generation programs. Nil, PO Box 7516, Berkeley, CA 94707.

Deadline for Spring Marketplace: 4/1/91.

PUBLICATION DENIAL NOTIFICATION

TITLE OF PUBLICATION 2600 Magazine Fall 1990 V7 N3

The above publication has been reviewed and denied in accordance with Section 3.9 of the TDCJ Rules and Regulations for the reason(s) checked below:

- ☐ (a) Publication contains contraband.
- ☐ (b) Publication contains information regarding the manfacture of explosives, weapons or drugs.
- ☐ (c) Publication contains material that a reasonable person would construe as written solely for the purpose of communicating information designed to achieve a breakdown of prisons through inmate disruption such as strikes or riots.
- ☐ (d) A specific factual determination has been made that the publication is detrimental to prisoner's rehabilitation because it would encourage deviate criminal sexual behavior.
- ☒ (e) Publication contains material on the setting up and operation of criminal schemes or how ro avoid detection of criminal schemes by lawful authorities charged with the responsibility for detecting such illegal activity.

REMARKS Pages 18, 19, 20, 21, 29, 42 and 43 contain information on misusing telephone equipment to make telephone calls illegally and to obtain cash and credit cards illegally. (Does not qualify for clipping.)

If there is a desire to appeal the rejection of the aforementioned publication, this may be accomplished by writing to the Director's Review Committee, P.O. Box 99, Huntsville, Texas 77340. The appeal must be mailed so as to arrive at the Texas Department of Criminal Justice, Institutional Division, within two (2) weeks of the date shown below

MAIL SYSTEM COORDINATORS PANEL

January 9, 1991
Date

2600 Magazine
Publisher / Sender

P.O. Box 752
Address

Middle Island, NY 11953
City, State, Zip Code

White
Canary
Pink

1193 Rev. 1/90

YOU CAN BET THIS WENT RIGHT UP ON THE WALL THE MOMENT WE GOT IT. WE'D LIKE TO KNOW WHAT OTHER MAGAZINES HAVE RECEIVED THIS HONOR. AND HOW MANY MAGAZINES CONTAIN CONTRABAND?

News for the week

Telecommunications security professionals, members of law enforcement organizations and public prosecutors may not be able to shut down computer data thieves if new advocates of hackers rights have their way. Support for Legion of Doom suspects developed as reporters following developments in the highly successful Operation Sun Devil crackdown listened to only one side--the hackers.

Apparently, the press got interested in digging into whether suspects' civil rights had been denied after Lotus 123 developer Mitch Kapor was approached by five attorneys complaining of overzealous enforcement tactics in Operation Sun Devil, the largest operation of its kind ever.

Kapor, who is president of On Technology, Inc., of Cambridge, Mass., responded by contributing $200,000 to a defense fund for alleged technopunks. Next, he formed the Institute for Computing Freedom, an apparent foundation for hackers' rights.

The highly respected American Civil Liberties Union got into the act after news reports of possible rights abuses surfaced in the Washington Post and New York Times. The result was that a June 9 Congressional Judicial Committee hearing on Caller ID matters was postponed so that hackers' rights can be addressed.

Rest assured that the hacker suspects will have highly articulate advocates at the hearing later this summer.

Assorted Numbers With Abuse On Them

- (800)225-0312 (PBX), two nine-digit codes; (800)535-4991, one five-digit code; (800)336-7800, one 10-digit code; (800)245-6332, three 10-digit codes; (800)843-3313, three six-digit codes; (800)327-9488, one 13-digit code; (800)248-8034, one six-digit code; (800)345-0017, six nine-digit codes; (800)962-4656, one six-digit code; Pheatures Newsline: (800)255-9679, box 262 and (800)877-5599, a number with high abuse by the hacker ORBID. (800)748-0375, Phillips Fibers, Inc.; (800)444-1333, (800)633-8256, (800)873-5669, (800)877-3444, (800)845-8856, (800)433-4467, (800)873-5666, (800)633-4102 and (800)535-6246.

- "Hackers are going after a carrier": (800)986-XXXX.

- PBX: (800)223-5517.

- 950-0511, three six-digit codes; 950-1022.

- Diverter: (800)422-7777.

- (313)980, plus the following mailboxes: Black Wizard, 8730; Mystic, 7760; Dark Side, 7558 and 7240; Phreak, 9077; Macho Man, 6846; Crocodile Posse, 4586; Sid, 7095 (personal box), 9157 and 5610 (Sid's codeline); Violator, 8839;5457 (codeline).

Fraud Alert, © 1990, Communications Fraud Control Association

THIS USEFUL NEWSLETTER IS AVAILABLE THROUGH THE COMMUNICATIONS FRAUD CONTROL ASSOCIATION, PO BOX 23891, WASHINGTON, DC 20026 OR 7921 JONES BRANCH DRIVE, SUITE 300, MCLEAN, VA 22102. (703) 848-9768

(continued from page 39)

shiny new penny with all of this garbage — by far the most valuable thing in the envelope.

***

By calling 1-900-USA-BUSH, you can delude yourself into thinking that you've sent a fax to the president! According to the telecommunications magazine TE&M, which really should know better, this service "provides every American citizen a personal 'hotline' to the president of the United States, George Bush, to comment on issues or pending legislation." Each call costs $7.95. The plus side is that you actually get something in the mail: a copy of the fax with a stamp of the president's signature. By the way, if someone can provide us with the *real* White House fax number, we'll print it. Your chances of actually having your message read by someone will be much greater and your phone bill will be much lower.

***

MCI has begun offering nationwide 900 service and seems determined to avoid the pitfalls of its predecessors. New 900 services must provide proof that their programs don't violate any regulations or telephone company policies. Advertising will be examined to make sure it's not deceptive. And MCI will insist that callers be notified of the price of the service and given enough time to hang up if they're not interested. Anything child-oriented cannot cost more than $4 total. And all adult-oriented services have to be on the same prefix so they can be easily blocked.

***

British Telecom now offers a service for its troops in the Persian Gulf to call home more easily. It's called "Desert Direct" and allows soldiers to reverse the charges for less than the direct dial rate. A time limit of 10 minutes is enforced to allow as many people as possible to use it. Meanwhile, Military Communications Corp. of Eden Prairie, Minnesota has opened three Phonecenters in Saudi Arabia, each of which has 144 phones. They will be able to carry more than 30,000 outbound credit card and collect calls every day. Military Communications Corp. also owns Phonecenters on military bases throughout the United States. And AT&T has set up a toll-free number for families that are having trouble paying their phone bill because of calls from Saudi Arabia (800-323-HELP).

***

In light of the recent AT&T failures where massive amounts of callers are unable to get through to 800 or 900 numbers because of computer problems or cable cuts, the geniuses in marketing have come up with a solution. "Alternate Number Translation" would store the customer's 800 or 900 number into a backup database. Then when AT&T's system fails yet again, AT&T would use the backup database to complete the calls. For $500 per number per month (plus a $500 setup fee), AT&T will try to keep its failures from affecting you. We'll be trying to find out the names and numbers of everyone who agreed to these terms so we can try to get some free money too.

***

If you're interested in a worthwhile 800 service, Cable and Wireless seems to have the best low-cost system. For $10 a month plus calls, you can have your own 800 number. For $20 a month plus calls, you can have a *programmable* 800 number. This is a great service for those of us who move around. Simply call a special 800 number, enter your code, and you can program your 800 number to forward anywhere in the country! The cost of the calls themselves are higher than directly dialed calls, but not by an obscene amount and far less than calling card calls. We think this is very useful for those of us with imaginations. Imagine what would happen if some rich entrepreneur-type set up his/her 800 number to forward to the White House! All of a sudden, every poor person in America would be able to get their opinion heard. (The White House doesn't accept collect calls nor provide any 800 service.) Technology in the hands of imaginative people can do wonderful things.

***

developments

Here's a reason to stay off the phone. Remember Telesphere, one of those companies that occasionally shows up on your phone bill asking for huge amounts of money for 900 numbers? Remember NTS, one of those companies that occasionally shows up on your phone bill asking for huge amounts of money for operator-assisted calls? They are now one.

***

"NYNEX is more than a family of companies, it is a family of people. We must be an ethical family. The only behavior that is appropriate for our businesses and for each of us, is behavior that meets our high ethical standards. There can be no compromise." So begins an internal memo from NYNEX encouraging its employees to rat on each other by calling 800-473-TALK from 9 am to 7 pm. After that they can leave a message on their hackable voice mail system at the same number.

***

Kevin Mitnick made news again when he was barred from attending a computer symposium in Las Vegas last autumn. The Digital Equipment Computer User Society says it never had a known hacker attempt to register for one of its symposiums before. Their hysteria fits right in with the media and government portrayal of Mitnick as the biggest threat known to computers. In retrospect, the crimes Mitnick was convicted of seem grossly out of proportion to the sentence he received: a year in prison, some of which was served in solitary confinement and without access to a telephone. This unfairness, along with Digital's panic at his appearance, will hopefully be seen one day as the absurd reaction of short-sighted individuals who let fear prevail over common sense.

***

Hungary is the first Eastern European country to get 800 service to the United States.... Ameritech, NYNEX, and BellSouth have all been granted permission to offer electronic telephone directories. It could be a great service if the cost is kept to a minimum.... Southwestern Bell is offering an electronic directory service called Directline Custom for large businesses. Each screen of information costs 9.2 cents and the charge for a user ID is $8.80. Oh yes, there's a one-time establishment fee of $4152. The service is located in St. Louis and is accessible via dial-up. AT&T will soon be offering the same service and it will be called "AT&T Find America".... Despite a lot of publicity, Pacific Bell's Message Center service can't seem to stop crashing. For the second time in a week in December, the "alternative to an answering machine" went down causing thousands of people to lose their messages. For four hours in the middle of the day, users couldn't access the system at all. Pacific Bell is still proud of the service, saying it's only failed a few times "not counting brief 2 am to 3 am kinds of outages". We don't know where they're coming from but we want no part of an "answering machine" that goes down for maintenance whenever it feels like it.... BellSouth claims to have become the first of the regional Bell companies to be completely electronic. No more crossbars, no more steps.... According to The New York Times, Bulgaria has become the breeding ground of "the world's most lethal computer viruses". Not only do they produce the most viruses, says a virus expert, they produce the best. Why is this? Apparently, a generation of Bulgarians has learned how to program but has no way of using their skills in society.... New York Telephone will soon be testing a "debit" card at New York City payphones. Money will be taken out of your bank account as you talk.

Too risky to mail?
Too paranoid to speak its name?
Then FAX it!
516-751-2608

DEFENDING HACKING

(continued from page 35)

have little or no understanding of what hacking is? Yes. Instead of being frightened by tall tales of hackers invading your privacy and taking over satellite transmissions and shutting down emergency phone systems, etc., I'm scared shitless over the *fact* that the government can kick my door in and take away my beloved computer because one day I called a bulletin board system that happened to be under surveillance for some random reason, or someone uploaded some sort of file to my bulletin board that I had no knowledge of. This can and has happened to innocent, unsuspecting people whose only crime was wanting to communicate with other computer users or download a public domain game.

Scenario: Joe Computeruser calls "The Gates of Eliteness BBS" one day hoping to get help on how to use his new spreadsheet package that he paid a large and legal sum of money for. He applies for an account and, as a result, his real name, age, address, and phone number (information that is required to gain access) are now stored in the BBS's user files. The sysop, Mr. Cool Joe Hacker, did something viciously maligned and has come under the scrutiny of the U.S. Government. His computer and all his files (and TV's, stereos, lamps, etc.) are confiscated, including the personal information of Joe Computeruser and countless other people who have accounts on the system. Joe Computeruser is now implicated in the investigation for collaborating in Mr. Cool Joe Hacker's exploits, along with the rest of the users on his BBS system, and is put under surveillance, even though he was calling for a most wholesome and legitimate reason. You don't think so, huh? Well, ignorance is bliss.

The government needs watching, not hackers. If hackers led the world, there wouldn't be half a million American troops in Saudi Arabia. Hackers don't send your sons and daughters to their deaths. The U.S. government does. While I cannot totally say "do not fear the hacker", I can say "fear the government".

After all is said and done, there is a limit. If a system exists that houses information, and you were not meant to be able to peruse that information then you do not have a constitutional right to be inside that system. But that's not to say that you won't go ahead and try to get into that system anyway. That's the choice you make, the rules of your game. There is such a thing as private property. That's one of the fundamental foundations our country is based upon. To use the argument that you have the right to be inside the computer systems of certain agencies gathering enormous amounts of information about you without your knowing, and to include in that argument that you have the right to be inside the computer systems of any private agency, company, etc. that houses information of any kind is not only entirely wrong, but stupid. But again, it all depends on the way the rules of your game are defined, the extent of your personal integrity, how screwed over you've ever been, and the way you look at life in general.

Since there will always be hackers, and there will always be those who think they have the right to be inside any system, the ultimate and unwavering responsibility lies on the owner of the system. If you don't make it secure enough, although you're not *asking* for someone to break into it (who would be?), you've got to realize that not everyone out there gives a shit, and by golly, if they want to hack into your system and they can, well then that's just what they're going to do. And that means that you overlooked something that you shouldn't have. That's life. That's the game.

If you enjoyed this issue, you may be interested in issues of the past. Move your eyes to the right for details.

HURRY UP

Time is starting to run out. 1991 is sure to contain lots of unpleasant things, but one of the worst will be a price increase for 2600 subscribers. We're not raising the price out of malice or because of some distant dictator. This is not a sneaky attempt to raise money for war bonds or terrorist activity. Simply put, we're increasing our price because our costs have gone up: postage, printing, and so on. The same old story. By renewing your subscription now, you can still take advantage of the old prices. Because next issue just won't be the same.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988,1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED: _____

internal organs

a political hacking scandal	4
the hacker reading list	8
central office operations	12
more leaked documents	16
anatomy of a rip-off	22
letters	24
winning reader entry	32
the word in the street	36
2600 marketplace	41
listings	42

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested