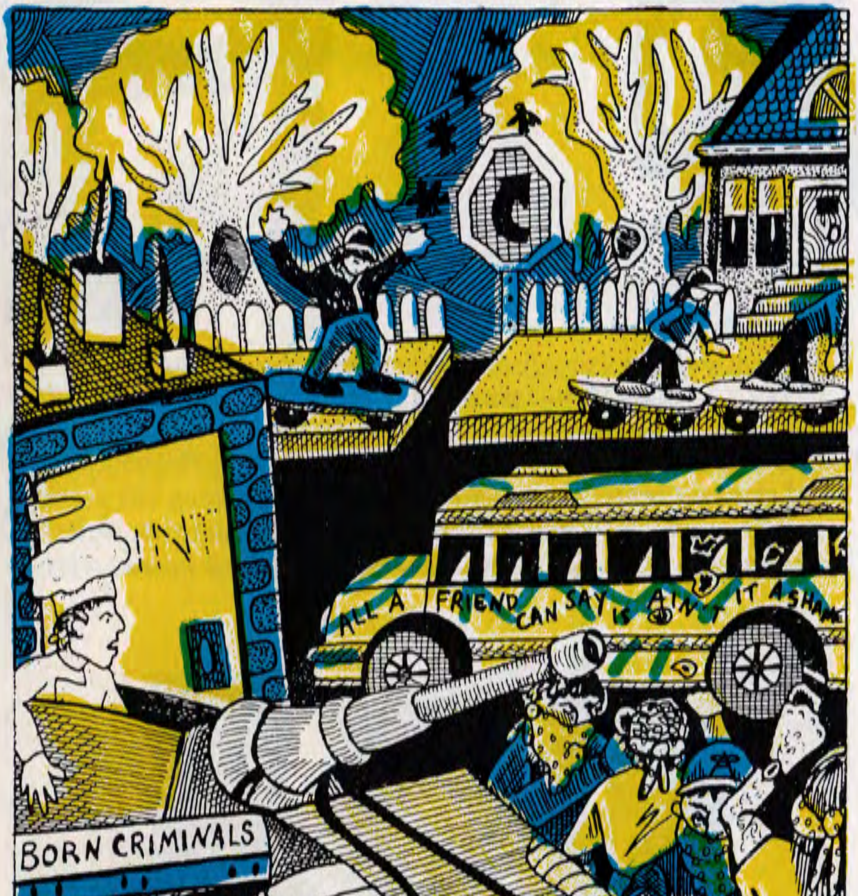
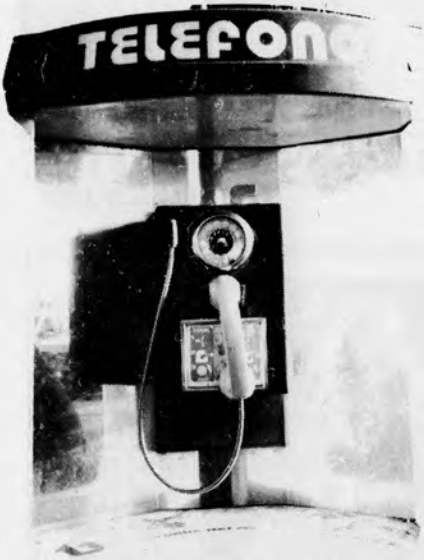
2600

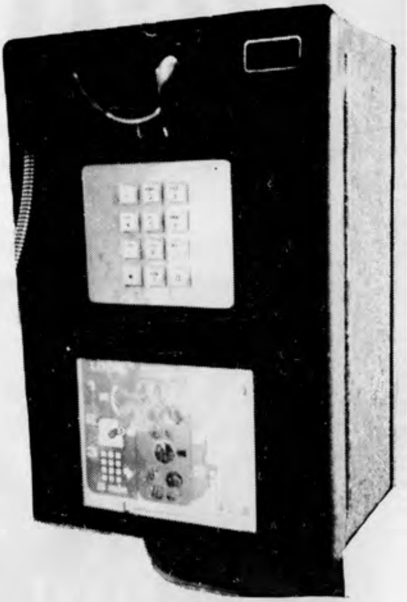
The Hacker Quarterly

VOLUME SEVEN, NUMBER TWO
SUMMER, 1990



MEXICAN PAYPHONES





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

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

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

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

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

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

A BITTERSWEET VICTORY

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

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

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

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

the neidorf/phrack trial:

by Gordon Meyer and Jim Thomas

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

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

The Trial: Day by Day

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

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

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

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

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

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

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

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

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

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

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

7. Female, Afro-American. Works in claims underwriting at CNA. Experience in word processing and using LAN based PC's. Former Illinois Bell and AT&T employee.

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

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

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

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

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

Alternate Jurors

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

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

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

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

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

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

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

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

the neidorf/phrack trial:

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

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

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

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

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

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

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

day by day

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

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

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

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

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

Credit Applications

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

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

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

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

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

(continued on page 40)

an interview with

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

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

Were you prepared to go to jail?

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

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

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

Were First Amendment issues ever raised at the trial?

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

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

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

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

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

Has it gotten better?

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

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

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

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

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

What are the plans for Phrack?

craig neidorf

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

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

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

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

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

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

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

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

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

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

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

Do you feel this was an accurate definition?

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

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

Don't let this scare you too much. It wasn't pleasant by any means. It's not something you want to have happen to you. Natural curiosity existed long before the computer was invented. It's something that you just can't eradicate. One thing I've learned from this is that being cooperative helped me tremendously at the trial. They asked me general questions and I didn't try to hide anything. But it's also possible that if they hadn't taken everything I said and manipulated it, perhaps there wouldn't have been enough to get me indicted in the first place. So I wouldn't say that it's necessarily all right to talk to these people if you have nothing to hide. I was tormented by things I had told them because of the way they interpreted it. It's not what you say, it's what they make out of it. For anyone else who gets a visit, don't lie to these people. But don't talk to them either, no matter how innocent you are. Get an attorney. I don't know if it would have saved me any trouble but at least they can't really make anything out of that because that's just a reasonable thing to do. To the hackers out there, I say fight for what you believe in. Obviously you don't want to jump in a situation and defend something you don't know enough about. You might be made to look foolish and you may find that you're wrong. I was defending the right to information. And I nearly went to jail for it. I hope that more people are prepared to fight as I was. When you accept a plea bargain on something this new, you're setting a precedent that's going to affect people down the road. Especially here, where they're going after kids who don't have the financial resources to defend themselves. Technically, I don't either. Had I plea bargained something out or plead guilty to something because it was the only thing to do financially, it would have set a precedent that could have done a lot of damage to other people in the future.

WHAT IS THE EFF?

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

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

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

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

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

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

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

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

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

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

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

NEGATIVE FEEDBACK

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

***

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

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

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

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

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

Privacy is a right held dear in the United States; it's wired into the bill of rights (search and seizure, due process, etc.) and into the common law. You will find that you can never convince people that hacking is harmless simply because it violates people's perceived privacy rights. It is one of the few computer crimes for which a clear real-world analogy can be made, and which juries understand in a personal way. That's why the balance has begun to tilt toward heavier and heavier sentences for hackers. They haven't heard society telling them to stop yet, so society is raising its voice. When the average hacker gets the same jail term as, say, the average second degree burglary or breaking and entering, and every hacker looks forward to that prospect, I suspect the incidence will taper off and hackers will find different windows to peep into."

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

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

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

***

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

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

***

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

FEEDBACK

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

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

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

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

***

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

Blecch.

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

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

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

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

We respectfully decline to do either.

***

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

My only quibble is that the 911 hack-

(continued on page 32)

PRIMOS:

by Violence

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

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

Primenet

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

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

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

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

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

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

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

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

■ Complete access and protocol

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

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

Checking Out a PRIMENET System

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

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

LIST_PRIMENET_LINKS - Lists PRIMENET status

LIST_PRIMENET_NODES - Lists configured PRIMENET nodes

LIST_PRIMENET_PORTS - Lists assigned PRIMENET ports

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

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

FIGURE A

```
OK, list_primenet_nodes

** VOID **

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

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

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

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

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

The PRIMENET RLOGIN Facility

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

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

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

NETLINK

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

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

WITH PRIMENET

- Other Prime's on the same PRIMENET ring as the system you are on.
- Any system (UNIX, VAXen, etc.) located on any of the world's networks.

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

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

OK, netlink

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

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

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

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

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

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

c <nodename>

An example would be:

c thrash

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

c <network address>

An example would be:

c 21398

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

c <dnic>:<network address>

An example would be:

C 2624:5890040004

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

5890040004 Connected

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

PRIME HACKING,

```
THRASH Connected
```

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

```
5890040004 Disconnected
```

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

```
5890040004 Rejecting   Clearing code = 0000
Diagnostic code = 0010 (Packet type invalid)
```

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

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

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

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

```
UUU@UUu
QUIT.
OK,
```

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

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

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

```
<cr>@<cr>
```

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

```
continue 1
```

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

```
prompt $
```

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

```
SET? 1:0,2:0,3:0,4:2,5:0,7:8,9:0,10:0,12:0,15:0
SET? 0:0,57:1,63:0,64:4,66:0,71:3
```

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

PART THREE

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

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

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

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

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

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

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

call <whatever> -fcty

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

continue 1

To connect to the second open circuit, type:

continue 2

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

Circuit does not exist

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

d #

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

d all

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

(continued on page 34)

AN INTRODUCTION

by The Plague

Introduction

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

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

COCOT Basics

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

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

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

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

TO COCOTS

echoing effects.

Identifying COCOTs

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

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

COCOT Varieties

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

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

Getting the Dialtone

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

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

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

REHABILITATING

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

COCOT Security Measures and How to Defeat Them

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

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

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

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

5) Number Restriction - Most COCOTs

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

Photo Salvation
Ken Copel

Design
Zelda and the Right Thumb

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

Remote Observations: Geo. C. Tilyou

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

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

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

Secret Numbers

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

Remote Connections

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

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

(continued on page 42)

Hunting for Wiretaps

Dear 2600:

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

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

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

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

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

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

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

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

San Francisco

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

Comments

Dear 2600:

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

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

Fred
Wilmington, Delaware

That yellow paper fades with age....

Dear 2600:

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

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

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

Milwaukee

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

On Government Raids

Dear 2600:

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

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

STM

Dear 2600:

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

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

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

DB

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

For the Record

Dear 2600:

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

The Acronym King

Questions

Dear 2600:

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

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

Simpson

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

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

Dear 2600:

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

BM

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

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

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

Dear 2600:

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

JI
Iceland

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

Dear 2600:

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

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

Jeff

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

Dear 2600:

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

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

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

Guerneville, CA

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

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

We don't have any BBS's nor can we recommend any as everyone seems to be in a state of paranoia. We can't emphasize *enough the importance of using bulletin boards to communicate freely, openly, and anonymously (when necessary). If you have the capability of running a board, we highly recommend it.*

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

Protection From Eavesdroppers

Dear 2600:

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

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

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

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

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

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

RG

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

2600 Compromising Ideals?

Dear 2600:

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

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

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

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

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

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

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

that letter today?

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

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

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

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

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

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

Disgusted Hacker

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

2600 letters, po box 99,

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

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

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

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

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

An Unusual Request

Dear 2600:

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

My name is Rick Saiffer, and that's part of the story for a screenplay I'm writing. I entreat *2600* readers to help make it realistic, creative, and especially devious. (In case you're wondering, the hero of this movie is a hacker who will eventually *discover* that the millionaire caused the crash, via sloppy hacking mistakes *he* made while *engineering* this crash!) I want the crash to be big: two 747's colliding in mid-flight over the Grand Central Parkway at rush hour would be delightful.

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

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

Free Phone Calls

Dear 2600:

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

Mr. Upsetter

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

Dear 2600:

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

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

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

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

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

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

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

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

Birmingham

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

NEGATIVE

(continued from page 13)

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

***

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

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

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

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

FEEDBACK

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

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

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

***

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

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

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

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

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

***

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

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

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

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

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

(continued on page 39)

HACKING

(continued from page 19)

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

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

Texts for Clearing Cause Codes detected by NETLINK

0 0 DTE Originated
1 0 Busy
3 0 Invalid Facility Request
5 0 Network Congestion
9 0 Out Of Order
11 0 Access Barred
13 0 Not Obtainable
17 0 Remote Procedure Error
19 0 Local Procedure Error
21 0 Out Of Order
25 0 Refusing Collect Call
33 0 Incompatible Destination
41 0 Fast Select Acceptance Not Subscribed
57 0 Ship Absent
128 0 DTE Originated (Non-standard Diagnostic)
129 0 Busy (Private)
131 0 Invalid Facility Request (Private)
133 0 Network Congestion (Private/Routethrough)
137 0 Out Of Order (Private/Routethrough)
139 0 Access Barred (Private)
141 0 Not Obtainable (Private)
145 0 Remote Procedure Error (Private)
147 0 Local Procedure Error (Private/Routethrough)
149 0 RPOA Out Of Order (Private)
153 0 Refusing Collect Call (Private/Primenet)
161 0 Incompatible Destination (Private)
169 0 Fast Select Acceptance Not Subscribed (Private)
185 0 Ship Absent (Private)
193 0 Gateway-detected Procedure Error
195 0 Gateway Congestion

Texts for Diagnostic Codes detected by NETLINK

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

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

Other Useful PRIMENET Utilities

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

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

OK, config_primenet configfilename

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

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

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

```
OK, monitor_net -ttp vt100
```

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

Miscellaneous Bits
The Physical System Console

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

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

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

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

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

OF PRIMOS

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

"One need not be malicious to learn."

Hacking Older (Outdated) Revisions of PRIMOS

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

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

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

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

Simplified Means of Attaching to Sub-UFD's

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

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

DOWN.CPL SOURCE CODE

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

UP.CPL SOURCE CODE

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

(continued on page 46)

NEWS UPDATE

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

NEGATIVE FEEDBACK

(continued from page 33)

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

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

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

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

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

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

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

phrack on trial

(continuedfrom page 7)

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

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

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

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

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

COUNTTWO

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

==Phrack Inc==

Volume Two, Issue 19, Phile #7 of 8

From The Creators Of Phrack Incorporated...

The Phoenix Project

Just what Is "The Phoenix Project?"

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

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

Why Is "The Phoenix Project?"

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

THAT DAY HAS COME...

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

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

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

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

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

Sorry for the short notice this year...

:Knight Lightning

"The Future Is Forever"

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

2600 Marketplace

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Deadline for Fall Marketplace: 10/1/90.

HOW TO MAKE COCOTS

(continued from page 23)

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

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

Getting the COCOT's number

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

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

Hijacking the Bastard

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

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

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

WORK FOR YOU

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

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

Destruction

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

The Phone Line

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

Advanced Techniques

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

Code Theft

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

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

Calling Card Verification

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

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

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

Call Forwarding

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

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

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

TO COCOTS

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

The Future of the COCOT

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

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

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

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

Getting More Info

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

Fighting the Bastards

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

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

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

PRIME CONCLUSIONS

(continued from page 37)

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

Conclusion

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

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

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

References

FDR3108-190L (PRIMOS Commands Reference Guide)

FDR3104-101B (New User's Guide to EDITOR and RUNOFF)

FDR3250 (PRIMOS Commands Programmer's Companion)

FDR3341 (BASIC/VM Programmer's Companion)

Hacking PRIMOS Volumes I and II (by Codes Master)

Hacking PRIMOS I, II, and III (by Evil Jay)

PRIMOS: Networking Communications (by Magic Hassan)

PRIMOS Part I (by Carrier Culprit, LOD/H Tech Journal #2)

PRIMOS (by Nanuk of the North)

Acknowledgements

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

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

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

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

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

***

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

IT'S SIMPLE

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

INDIVIDUAL SUBSCRIPTION

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

CORPORATE SUBSCRIPTION

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

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

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

BACK ISSUES (never out of date)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25 □ 1989/$25

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

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

TOTAL AMOUNT ENCLOSED: □

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