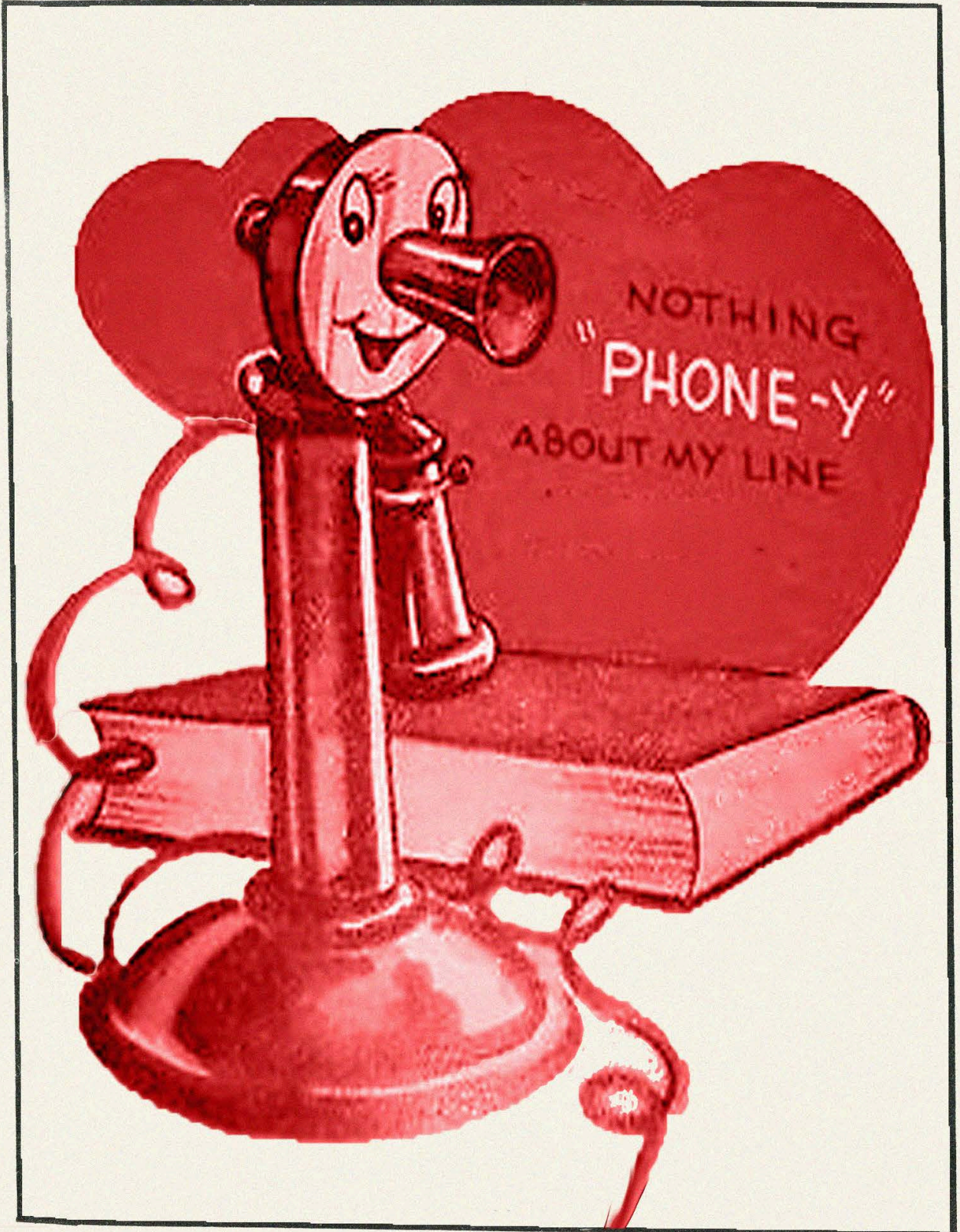


2600

The Hacker Digest - Volume 5

1988



CHANGES

1988 was when we finally settled into our quarterly schedule, which would become an essential part of *2600* from that point on. In fact, we christened ourselves “The Hacker Quarterly” with the very first issue that adopted the new format: Spring 1988.

The page length of each issue was doubled to 48 pages. Page numbers appeared on pages 2 through 47 in the Spring issue and from that point onwards pages 3 through 46 as the inside covers no longer had labeled page numbers. We continued to print in color on the front and back pages. As in 1987, the back page was devoted to the table of contents and was simply labeled “CONTENTS.” The words “DANGER: MISSING LABEL” appeared in the spot where the mailing label was supposed to be affixed for those people who had opted not to get the magazine in an envelope. (In 1987, the phrase had been “WARNING: MISSING LABEL.”) The Winter 1988-89 issue was formatted a little differently on that page. Instead of the missing label notice, a different message was printed over to the left in really tiny print. Those with microscopes or really good vision would see the message: “When Was Your Last Eye Exam?”

COVERS

The first two covers were done by cover artist Ken Copel and the last two were photographs. We continued to use our little box in the upper right hand corner as a mini-cover for various messages and bits of art.

Spring 1988 featured an image of a guy sitting on a huge computer monitor talking on a telephone. His words “No, it’s safe. You can talk.” are displayed on the screen for all to see. The computer, of course, is a Model 2600 of one thing or another. Our mini-cover was the buffalo image of a standard 22-cent postal stamp upside down. We were a little curious if this might somehow cause issues with postal machines processing our magazines. This was also the only cover of the year that had the price (\$4) of a single issue for newsstands printed on all issues. For subsequent 1988 issues, we managed to only print the price on those issues that were being sold in stores. (If you have one of those, it’s particularly rare.)

The Summer 1988 issue had an interesting view into the insides of a computer from the back where you could see an inverted message on the screen along with the image of a city either beyond that or contained as part of it. The partially obscured message read: “When there is no tiger upon the mountain, the monkey shall be king. :2600 Sends.” Other than the “2600” part, this was an old Chinese proverb. Also hidden in the image is our ISSN number just for kicks. Our mini-cover featured a full screen close-up of President Ronald Reagan pointing to the part of his nose that had skin cancer. It seemed relevant at the time.

Autumn 1988 was a bit different as it was simply a reprint of a photograph we had obtained from Bell Labs that demonstrated how specially designed computers could manipulate pictures and create unique and seamless images. This was one of very few covers that did not come from in-house. Our mini-cover, however, most certainly did. What looks almost unidentifiable was actually a very clear message - if you knew what to look for. Back in 1984, in our first issue, we exposed an FBI informant who was targeating hackers. Our article back then thwarted much of his work, but he continued to strike at people close to us, all the while claiming he was untouchable. We managed

to track down much of his hidden information but, rather than just let loose with a barrage of harassment, we felt a little demonstration would be more effective. So, if you turned that little image on its side, you would see the front of the informant's office in Detroit, an address that had remained fairly unknown. We imagine the message was sent, as the harassment stopped soon after. Probably the most fun we ever had with a mini-cover that nobody else, save one other person, understood. Until now.

Winter 1988-89 was our final cover of the year and, again, it was from an external source. It was an ancient photo of a payphone booth from 1884 touched up in blue. A caption underneath identified it as part of the "National Telephone Company" (England) and revealed the rates of the time. An excerpt of their original literature was reprinted on the next page. The mini-cover somehow managed not to stay in the box and was a simple curved meter with a word printed underneath. The word? Bushitera. This was apparently a reference to the recent election that voted in George H.W. Bush. So instead of a bullshit era, we were about to launch into a Bushit era. It seemed so much more clever at the time.

INSIDE

The staffbox continued to appear on page 3 with Emmanuel Goldstein now listed as Editor-In-Chief. Other listed credits at various times of the year were Office Manager, Production, Cover Art, Artwork, and Writers.

Mailing info also appeared on page 3 for each issue. We had three BBSes listed in Spring (OSUNY, Central Office, and a nameless third one) and four beginning in Summer (Yoyodyne as the third and Beehive as the fourth). The Winter edition introduced a fifth BBS (Hacker's Den) and saw OSUNY listed as "down at the moment."

Somehow we managed to say we were "published monthly" in the Summer and Autumn issues after getting it right in Spring. This was fixed for Winter.

The pursuit of advertising was abandoned this year. Exceptions were confined to our own house ads and reprints of advertising that we found to be amusing or crazy.

We were happily surprised to come upon some decent and positive press concerning hacking over in England, in the form of a television program titled *Network 7*. "It's possible the press is finally growing up and realizing that hacking involves so much more than electronic bandits. It's a symbol of our times and one of the hopes of the future. If that sounds crazy to you, wander through our pages and it may start to make sense."

In following mainstream news, we were always keen to point out how elusive privacy actually was by default with warnings like "one should not presume that a long distance telephone call is private." Regarding the existence and future of telephonic spying by the authorities, "It's doubtful that one system could spy on numbers across the country because of the many different systems still in use. If and when all of the phone networks become integrated, such a concept will be very possible." Rumors abounded about a monitoring device known as a REMOB, for which we offered a \$100 reward for any evidence that proved its actual existence.

Our warnings about blindly accepting technology yielded some specific examples at a local university that had just installed a ROLM telephone system. "It is vital not to be dependent on any form of technology because

when it fails, you will be crippled,” the article emphasized. “Complete and total integration. Complete and total paralysis,” it concluded.

We got a fair amount of criticism for printing an “interpretation of computer hacking” that was far from positive. But we had wanted to stir the pot and create a dialogue and we certainly got that and more. We also were chastised roundly for devoting a huge amount of space in the Summer issue to the topic of computer viruses, particularly one article that focused on a specific bit of anti-virus software. However, we also printed an unapologetic piece from an actual virus writer which the readership was much happier with. “To write and distribute a virus you must lose every shred of moral fiber, and if I know the readers of this magazine, there will be a computer virus plague in the very near future.” (Speaking of plagues, the writer used the handle of “The Plague,” which would one day be incorporated into the movie *Hackers*.)

We printed some documents we obtained from The Private Sector raid of a few years back that amply demonstrated what a huge waste of time it was for the authorities to move against our first BBS. But we also tried to focus on the positive and on the power that those same authorities were so afraid of: “Every kid going to school today that has a computer and a printer in his home or even in his school is a potential newspaper editor.”

We even looked at the various candidates running for president in 1988 in terms of their attitude towards technology and concluded: “Representative Albert Gore showed himself to be the most knowledgeable ‘telecom enthusiast’ seeking the nomination.”

It was in the spring of 1988 that we decided to make 2600 meetings monthly instead of weekly, which seemed to synch well with making the magazine quarterly instead of monthly. It was the year that we printed our first red box plans. For the second time (the first being in 1987), we printed a photo of a foreign payphone, this time in Paris. We still didn’t realize what a good idea that would turn out to be.

Telephony was much more of a focus in this period. While we still yearned for a way to reach people “around the globe” through technology, we seemed to have the most fun continuing to play with the telephone network. The holy grail of any phone phreak was an unrestricted dial tone and we were chock full of tips on how to find them. Mischief was at the heart of it all: at one point we were helping to spread Moral Majority cofounder Jerry Falwell’s 800 numbers far and wide. It was an early form of hacktivism to overload these numbers and have his organization foot the bill as well.

We did our share of reporting on the phone companies too. We helped publicize a class action lawsuit against Allnet and exposed some Sprint billing issues. Apparently, they were charging for busy signals and splitting large calls into multiple smaller ones, yielding higher bills since the first minute of each call always cost more. They even were caught harassing people to pay bills that hadn’t arrived yet and, when they did arrive, these bills would often show several months of activity instead of only one. It was a difficult period for these new companies and we sure weren’t showing them any mercy. MCI really earned our wrath by signing up customers who hadn’t chosen them as their long distance carrier (a procedure the entire country was going through for the very first time). But probably our true rage was reserved for companies known as Alternative Operator Services (AOS), which quickly earned a reputation as horrible rip-offs, often charging many times the normal rate for a phone call, all the while fooling the customer into thinking they were using a more legitimate company. Again, we implicated MCI in this, as they facilitated the acceptance of AT&T calling cards on their network,

but routed it to an AOS company known as NTS, which resulted in huge and surprising bills to many. We printed pages of our own bill to demonstrate the issue.

We also were enthusiastic about coming changes, such as the introduction to our mechanical crossbar switch of something known as an adjunct frame, which would allow us to do such newfangled things as choose a long distance company and make international calls without the help of an operator. We wondered what the future of area codes would be, as only five of the traditional kind (with one or zero as the middle digit) were left. We had ideas for unique uses of the feature known as call forwarding, some of which are quite common today. And we watched as the total number of available cell phone channels went all the way up to 832. Meanwhile, a legendary payphone robber known as James Clark was finally captured after traversing the nation emptying coinboxes.

We saw the first instance of the Electronic Communications Privacy Act (ECPA) of 1986 being used to protect the private email on a BBS. And we had some classic quotes, including: "A simple human being... should be the one running the show"; "...it's becoming increasingly common for the installers of such systems to blatantly disregard the needs of the users and just assume everyone will figure it out in the end"; and "one must use good sense when entering a manhole." One particularly telling response to a letter summed our feelings up in this manner: "Computers still offer a degree of anonymity. Let's all try to enjoy that while we can."

We confronted some ugly feelings in the hacker community in the form of an anti-gay comment in a list of phone numbers we printed. We opted to keep the comment in, with this added: "2600 Note: We thoroughly deplore ignorant and prejudiced statements like this one and hope most of our readers do too. We decided to keep it in this list to face up to the fact that the hack/phreak world has its own redneck element." Needless to say, this didn't meet with universal approval, but we defended our actions, saying: "Racism and its assorted relatives thrive when people try to deny their existence. Computer hackers are not immune from any of this. We can only hope that they, along with most of the others in the world, will look for injustice and scream about it when they find it."

1988 was the year we first introduced 2600 t-shirts, which apparently was so unexpected that we had to add "no, we're not kidding" to our announcement, along with the warning of "no returns regardless of what you say or do." Nobody dared try.

The end of the year saw the first reports of the infamous Internet worm created by Robert Tappan Morris. And as the absurdity of the ECPA's restriction on listening to certain radio frequencies became apparent, we chose to print the transcripts of overheard conversations from insecure cellular telephones. The year ended with an interview of members from an intriguing group of people in Germany known as the Chaos Computer Club. "When a byte somewhere goes wrong," they told us, "they always phone the Chaos Computer Club, because they think we can fix it or we know what has happened and who did it." This was something we could identify with, but there were some things we just couldn't understand, such as this remark from the Germans: "If you need a longer cable you have to go to the post office and pay 65 marks and fill out a request form for a longer cable to your telephone."

And with all that, The Hacker Quarterly finally finished its first year.

2600

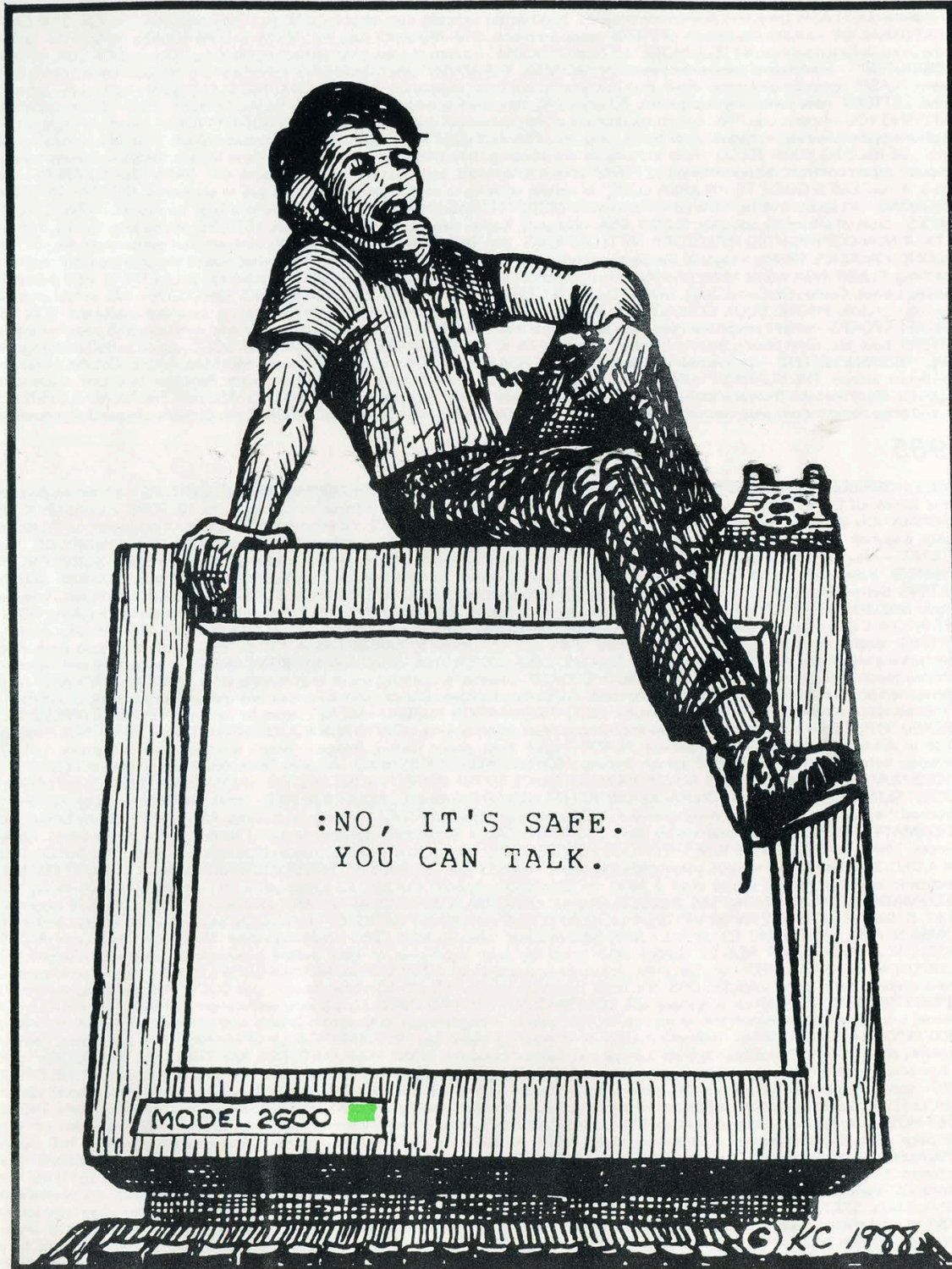


The Hacker Quarterly

Volume 5, Number 1

Spring, 1988

\$4



DO YOU HAVE BACK ISSUES OF 2600? If not, look what you're missing!

1984

AHOY!—an introduction to 2600; FBI GOES AFTER ADS HACKERS—FBI investigator unwittingly reveals tactics and recent activities; FLASH: LICA discusses GTE raids, AT&T credit cards, wireless phone trouble; THE TRUTH BEHIND THOSE 9999 NUMBERS—a toll free error story; DATA: various White House extensions; HACKING ON TELENET—how to's of Telenet use; ESS: ORWELL'S PROPHECY—the first in a series on the fun and dangers of ESS; FLASH: directory assistance changes, computer air-ban, AT&T credit cards, etc.; SOME THOUGHTS ON GARBAGE PICKING—first of a series of trashing for valuable information as related to a discussion of crosstalk; DATA: COUNTRY CODES—every last country code for overseas dialing; THE CONSTITUTION OF A HACKER—a discussion of hacking; ALTERNATE LONG DISTANCE: MCI—history, systems, and services; FLASH: 718, Connecticut wiretaps, Sweden person numbers, etc.; THE FIRST ATOMIC BOMB—an inside story on the event as related to our nation's phone system; DATA: ARPANET HOSTS—list of accessible hosts; WHOSE STRIKE WAS THAT ANYWAY?—a startling analysis of summer 83 phone strike; THE TROUBLE WITH TELEMAIL—discussion of GTE's irresponsibility in protecting their system; FLASH: AT&T credit cards, portable prisons, 414's plead, etc.; A TRUE SAGA OF TELECONFERENCING—what can happen on a teleconference; DATA: MCI ACCESS NUMBERS—DIALUPS FOR MCI MAIL; PHONE BOOK COLLAGE #1—our artistic heritage in phone book designs; THE SIMPLE PLEASURES OF A STEP OFFICE—discussion of ins and outs of antiquated phone systems; IBM'S AUDIO DISTRIBUTION SYSTEM—using voice messaging technology; FLASH: 414 sentencing, equal access, bank record privacy, etc.; THE WOES OF HAVING A SMALL-TIME RURAL PHONE COMPANY—a true story; DATA: AVAILABLE NETWORKS ON THE DEFENSE DATA NETWORK—a list including base addresses; EASYLINK ACCESS NUMBERS; ARPANET HOPPING; AMERICA'S NEWEST PASTIME—how it works and tips for its use; ELECTRONIC SWITCHING ADVANCES—some of the possible services and drawbacks; FLASH: Directory assistance charges, 2600 writer indicted, demise of E-COM, etc.; THE DARK AND TRAGIC SIDE OF THE GREAT BREAK-UP—a frank discussion; LETTERS: sysop problems, 518-789 an XY step, etc.; DATA: E-COM ACCESS NUMBERS—dial ups for the (now-defunct) service; NY TELEPHONE "LETTER OF DOOM"—a copy of a law enforcement monitoring notice; "LOOK OUT, HE'S GOT A COMPUTER!"—a defense of the hacker viewpoint; MCI MAIL: THE ADVENTURE CONTINUES—an analysis of the well-known faulty E-mail system; FLASH: computerized meter-maid, blue box arrests, anti-hack legislation; INTRODUCING THE CLEAR BOX!—"post-pay" payphone device; LETTERS: new switching equipment, 99 scanning, repulsive operator story, etc.; SPECIAL REPORT: TRW—BIG BUSINESS IS WATCHING YOU—how to use TRW, and an assessment of the potential of this system; BUT HOW DOES IT WORK?—a simple explanation of the phone system, wiring, voltages, black boxes, ring, etc.; PRIVACY LOST—a review of David Burnham's book "The Rise of the Computer State"; BE NICE TO YOUR TELCO—how individuals are abusing their telcos; FLASH: Big Brother in Miami, NASA computer break-in, computer export controls, 800 directories; LETTERS: phone scramblers, page numbers, hacker's book, etc.; DATA: CNA NUMBERS—list of CNA's; A HACKER'S GUIDE TO AN AREA CODE—a simple scheme to help "map out" exchanges in your area; HISTORY OF BRITISH PHREAKING—an account of the history and techniques; MORE ON TRASHING—what to look for, where to go, how to act; A FRIEND IN HIGH PLACES—story of a friendly operator; FLASH: NSA insecurity, hacker caught, private directories; LETTERS: phone loop, WATS, TAP, etc.; DATA: A NON-COPYRIGHTED DIRECTORY; NY TELEPHONE "BIG BROTHER" LETTERS—touch tone without permission, etc; GETTING CAUGHT: HACKER'S VIEW—a story of the personal effects of hacking; VITAL INGREDIENTS—what makes the phones work: operators, switching; FLASH: NSA wants better phones, crime-computer victim, wiretap loopholes, 911 attacker caught; LETTERS: BBS discussion, Comsec Letter, Computer Crime Data, others; DATA: NY TELEPHONE SECURITY NUMBERS; MCI ANECDOTE—ads, vulgarisms, MCI chairman profile; PHONE BOOK COLLAGE #2; EXPLORING CAVES IN TRAVELNET—an interesting extender explained; FUN WITH FORTRESS FONES—what a pay phone does, how people beat them; FLASH: SS computer foul ups, Airfone, wiretaps, 818, pay phone attack; LETTERS: book list, silver boxing, another hacker's view; DATA: IC'S AND CARRIER IDENTIFICATION CODES—guide to 950 exchange; MCI MAIL "TROUBLE LETTER"—the harassment begins; A TIME FOR REFLECTION—the year in review; MCI MAIL AND EASYLINK—electronic mail horror stories; THE SCARIEST NUMBER IN THE WORLD—true story; FLASH: campaign computer, Pentagon by phone, students bog computer, electronic jail, federal phone upgrade; SURVEY—reader survey responses; SOME, BUT NOT ALL ELECTRONIC MAIL SYSTEMS—list and price comparisons plus voice messaging companies; REACH OUT AND GOOSE SOMEONE—list of many unique dial it numbers.

1985

THOSE HORRIBLE HACKERS STRIKE AGAIN—analysis of Newsweek incident; WIRETAPPING AND DIVESTITURE—a Lineman discusses these topics; GETTING IN THE LACK DOOR—a guide to some popular operating systems including TOPS-10, TOPS-20, and UNIX; 2600 INFORMATION BUREAU: our phone bill, our thanks, and other notices; FLASH: IRS and telco data, GEISCO, KKK computer; LETTERS: BBS rights, Easylink, Canada loops, international phreak day; BITNET TOPOLOGY—a schematic of the BITnet; THE THEORY OF "BLUE BOXING"—history, future, and how they are used; TRASHING ALASKA STYLE—a real trashing adventure story; SURVEYING THE COSMOS—a beginner's guide to COSMOS, Bell's computer program; FLASH: phreak roundups, real TRW crime, 2600 BBS, 800 data; LETTERS: Bell problems, telco discount, marine calling, many questions; 2600 INFORMATION BUREAU—acronym list of useful telephone jargon; NAZI BBS A CHALLENGE TO HACKERS—the role of the hacker; ARE YOU A PHREAK???—humorous review of phreaking; HOW TO GET INTO A C.O.—a tour of a central office; FLASH: custom calling, Kenyan pay phones, hacker coke machine, IRS computer screw-up; LETTERS: reading list, tracing and law enforcement, UNIX info, NSA phone #; 2600 INFORMATION BUREAU—interesting phone numbers, how to dial a telephone, New York Tel message, CNA LIST, NSA CIPHER DISK, WHAT A WHITE BOX CAN DO—how to build and the use of a portable touch-tone generator; A PHONE PHREAK SCORES—another successful social engineering story; HACKING PACKARD—useful information about the HP2000; FLASH: talking clock, computers for communists, robot kills man, war games, silver pages; LETTERS: Tom Tompidis, secure telephones and cryptography; 2600 INFORMATION BUREAU—MILNET hosts by location, PEOPLE EXPRESS TO BE HACKED TO PIECES—a look at People's new anonymous reservation service; HOW TO RUN A SUCCESSFUL TELECONFERENCE—complete guide to Alliance Teleconferencing Service; FLASH: hacker bust, police hacker, Reagan doesn't dial kids, dial-a-directory; LETTERS: computer networks, silver boxes, 950, remob, tracing; 2600 INFORMATION BUREAU—Alliance Teleconferencing material; INTERESTING PHONE NUMBERS; UNBELIEVABLE ADVERTISMENT; GUIDE TO THE ISRAELI PHONE SYSTEM, SHERWOOD FOREST SHUT DOWN BY SECRET SERVICE; SOME WORDS ON HACKER MORALITY, OUT OF THE INNER CIRCLE REVIEWED—an ex-hacker's new book; FLASH: who invented the phone, porno phone, wiretap award, AT&T computer steals; LETTERS: information charges, AT&T cutoff, marine calling; 2600 INFORMATION BUREAU—800 prefixes by state, SYSTEMATICALLY SPEAKING: goodbye to meter readers, Thai phone books, tracking devices, TINA, "Call Me" Card; FROM SHERWOOD FOREST: INTRO TO HACKING—what to do and not to do; INTERESTING THINGS TO DO ON A DEC-20—how to use various commands and some things to look for; BANKING FROM YOUR TERMINAL. A LOOK AT PRONTO—Electronic banking, how it works with a focus on Chemical's system; FLASH: \$2 billion error, ITT crackdown, monitoring; 2600 INFORMATION BUREAU—Milnet TAC dialups by location; SYSTEMATICALLY SPEAKING: MCI goes optical, 100% ESS, GTE bigger than AT&T; SEIZED! 2600 BULLETIN BOARD IS IMPLICATED IN RAID ON JERSEY HACKERS—an accurate account of the Private Sector BBS; COMMENTARY: THE THREAT TO US ALL—what BBS seizures mean; FLASH: 2600 a hacking victim, Middlesex Courthouse, MOVING SATELLITES, WHAT WAS REALLY GOING ON?—point by point correction of New Jersey prosecutors' fallacious charges; WHY COMPUTERS GET SNATCHED—why law enforcement seizes equipment; SOME IMPORTANT QUESTIONS TO ASK—provocative questions about these events; HOW CAN SYSOPS PROTECT THEMSELVES?; A GUIDE TO VMS—how to use DEC's VAX operating system; THE INFINITY TRANSMITTER—an old bug explained; REACHING OUT ON YOUR OWN—blue boxing verification; PURSUIT FOR PEOPLE—GTE Telenet's computer to computer link-up service; FLASH: phone-in registration, 800 word numbers, war game addict, hacker extortionist; 2600 INFORMATION BUREAU—Telenet directory of interesting addresses; SYSTEMATICALLY SPEAKING: Dick Tracy toys, computer directory assistance, Bell propaganda films, Europe standardizing telcos; MANY FAMILIAR TONES, AND THEY CALL US CROOKS?—story of a phone phreak who can't sell his expertise; AN INTERESTING DIVERSION—call diverters and how they are abused; MORE INFO ON VMS—second installment of an in-depth guide to VMS; FLASH—computer elections, big phone bill, Navy phreaks, phone booth captures man; LETTERS: BBS suggestion, colleges are a goldmine, recommended reading; 2600 INFORMATION BUREAU—Blue Box plans; THE NEW AT&T HOSTAGE PHONE—unbelievable ad; SYSTEMATICALLY SPEAKING: hackers scare businesses, DuPont bypasses telco, computer campaign info, phone computers, divestiture woes; RSTS: A TRICK OR TWO—some aspects of this operating system; THE SECRET REVEALED—the problem with GTE's GTD#5 switch; HISTORY OF ESS, EQUAL ACCESS MAY NOT BE "EQUAL" TO MODEMS—some problems that may arise; FLASH: columnist attacks AT&T, feds dial-it too much, little town phones, Springsteen mania; LETTERS: some advice, CIC's and free calls, British phreak, blue boxing gone?; CHASE BANK IS CRACKED; 2600 INFORMATION BUREAU—many interesting test numbers; SYSTEMATICALLY SPEAKING: avoid phones in storms, rural unequal access, police cellular phones, toll-free from where?; AT&T to read e-mail; OUR WISHES FOR '86 AND BEYOND—some of what we'd like to see in the future; FUN WITH COSMOS—how to interpret and use parts of the phone company computers; FLASH: French phones, racist banter, Cityphone; SURVEY—reader survey responses; 2600 INFORMATION BUREAU—BBS numbers; SYSTEMATICALLY SPEAKING: AT&T e-mail, German phones, super pay phone.

(continued on inside back cover)

Spring has arrived. And this is the spring issue of 2600. Our new quarterly format has allowed us a bit more time to put together a more cohesive magazine. We hope you're pleased with the result.

Never before have so many pages been printed in a hacker publication. There are so many topics to discuss that are relevant to our "cause". In this issue, you'll find pieces about disastrous telephone systems, the effects of becoming dependent on computers, ways of eavesdropping on telephone

calls in such a way as to be completely undetectable, additions to our previous articles on IBM computer systems, and an interesting look at the world of phone phreaks and computer hackers which contrasts with the way we actually see ourselves. Plus all kinds of numbers, codes, displays, and reproductions that ought to make it all more interesting.

We've got so much to say and an increasing number of ways to say it. Our larger but less frequent schedule gives us both the time and the space we need.

(continued on page 8)

STAFFBOX

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Bobby Arwatt

Production
Mike DeVoursney

Cover Art
Ken Copel

Writers: Eric Corley, John Drake, Mr. French, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOC, David Ruderman, Bernie S., Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright © 1988, 2600 Enterprises Inc.

Yearly subscription: U.S. and Canada \$15 individual, \$40 corporate.

Overseas \$25 individual, \$55 corporate.

Back issues available for 1984, 1985, 1986, 1987 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.

2600 Office Line: 516-751-2600

BBS #1 (OSUNY): 914-725-4060

BBS #2 (CENTRAL OFFICE): 914-234-3260

BBS #3 402-564-4518

USENET ADDRESS: 2600@dasys1.UUCP

ARPANET ADDRESS: phri!dasys1!2600@nyu

monitoring phone calls

This public domain article, written a couple of years back, was obtained from ARPANET. It goes into technical detail on receiving microwave linked telephone conversations using conventional and widely available ham satellite equipment and/or plain satellite TV receiving equipment. Our thanks to the subscriber who sent it in. Regretfully, we don't know who originally wrote the article.

Now that Congress has chosen to attempt to patch a massive hole in the security of communications in the U.S. with a badly drafted law that does not require or even encourage carriers to implement solutions that actually increase real security, I thought I would repost an article I wrote a year ago about a major aspect of the real problem. I hope by so doing to remind everyone that even with a draconian law in place it is still very easy to intercept many regular telephone calls and data circuits.

Nothing in the Electronic Communications Privacy Act of 1986 requires or even particularly encourages carriers to increase the security of radio or satellite links. Listeners who get caught can be punished, but nothing has been done to make listening harder.

The kinds of interception I describe are now highly illegal under the new law, but the equipment required is very widely available (and has important legitimate uses that make a ban on sale or possession very unlikely) and the act of interception can be carried out in total secrecy and is nearly impossible to detect from a distance. The justice department has stated that they do not intend to seriously enforce the radio portions of the law which have been generally recognized to be unenforceable even by the bill's sponsors. So the law, while draconian, really won't have much of a deterrent effect even as respects casual listeners. And casual listeners are not the real problem.

Yes, it is possible, and not even very difficult.

Some years ago it was pointed out that 68 percent of long distance telephone trunks went by ground based microwave. And while the long distance carriers have been working (under some pressure from the NSA and White House) to convert these circuits to optical fibers or at least coaxial cable there are still many routes that use microwave or satellite hops. I don't know an

exact figure but I think it would be reasonable to guess that at least 40-50 percent of long distance trunks include a microwave or satellite hop. And some 75 percent (approximately) of long haul microwave relays use the 3.7-4.2 Ghz band which is readily receivable by a TVRO.

Most long haul microwave systems use FM modulation and frequency division multiplexing (FDM) of single sideband suppressed carrier voice channels. Some satellite systems also use this modulation. Unfortunately, FM-FDM-SSB modulation is quite easy to receive with simple and widely available equipment. Recovering the contents of a specific channel is very easy, which opens up the possibility of monitoring random phone calls to a specific group of destinations or monitoring specific private line data or voice circuits (which are assigned to a multiplex slot for long periods of time).

The question of whether a TVRO could be used to monitor phone conversations has been raised on the net. The answer is that with the addition of a stable general coverage single sideband receiver (such as an ICOM R-71 or a Kenwood R-2000 or the receiver section of a modem transceiver) connected to the unfiltered and unclamped video output (provided for connecting stereo adapters and descramblers), a TVRO can be used to listen to FM-FDM multiplexed telephone signals from both celestial and ground-based sources.

Further, with a stable down block down converter that converts to the UHF TV band and one of the scanner type receivers designed to cover this band, one can also receive some of the single channel per carrier (SCPC) signals that carry telephone circuits to more remote places (along with network radio feeds, Muzak, and various broadcast data services such as the AP and UPI news services). (Some signals are dithered and require some form of closed loop AFC to receive them.)

This vulnerability has been well known in security circles for many years, but as the number of TVRO systems has increased to over a million, the problem assumes a somewhat different perspective. In 1976 Mitre estimated that it would cost \$50,000+ to intercept microwave telephone calls, and would require a 10 foot dish. In that era a 10 foot dish would

with a TVRO

attract much attention. Today one can buy a TVRO system with a 75k LNA and an 8-12 foot dish for \$1000-\$1500, and almost nobody will give the system a second glance as TVRO's are commonplace. A 75k LNA beats the 10-12 db noise figure receiver that Mitre based its calculations on by a very substantial amount. And the current generation of computer controllable general coverage SSB receivers are much cheaper demultiplexing devices than the synthesizer and selective voltmeter that seemed necessary in 1976.

"One should not presume that a long distance telephone call is private."

The existence of all these millions of receivers that can pick up both celestial and ground-based telephone circuits means that one should not presume that a long distance telephone call is private. And more important (because they are much easier to find in FDM complexes), nobody should assume that a private leased line is secure (unless the long distance carrier has specially routed it via lightwave (much more secure) or coaxial cable (somewhat more secure) for its entire path. (Obviously conventional wiretaps also have to be considered if there is some reason to believe that some individual or organization has a strong enough reason to be interested in your communications to take the risks involved in actually physically tapping your lines.)

Background

Communications satellites carry telephone traffic in several formats. The principle formats are:

Multi Channel systems

1. FDMA-PSK-TDM-PCM.

Used on a number of transponders on 4 and 12 Ghz satellites. Heavily used by private business for tie lines and other leased line services, sometimes mixed with data. Quite secure if encrypted. Not easily intercepted by private individuals.

2. TDMA-PSK-TDM-PCM.

Used on SBS (12 Ghz) satellites as the principle access technique. Therefore SBS Skyline service and some MCI service (they are now both owned by IBM) is protected this way. Used also on some 4 Ghz transponders. Very difficult for private individuals to intercept even if not encrypted. Some circuits are encrypted, some not. TDMA is felt to be the heavy use satellite access technique of the future as it offers very efficient use of transponder power and dynamic allocation of system capacity to those links which are currently active. When combined with encryption it is quite secure.

3. FDMA-FM-FDM-SSB.

Standard modulation used on almost all terrestrial long haul telephone microwave circuits. Used on several 4 Ghz domsat transponders and most older multi channel Intelsat links. Wideband FM-FDM signals can be readily received by standard TVRO receivers, and an individual channel can be easily picked out of the multiplex signal with a garden variety general coverage SSB communications receiver. Very easy for private individuals to intercept.

4. CDMA-TDM-PCM, otherwise known as spread spectrum.

CDMA or spread spectrum techniques are widely used on military satcom links because of their security and resistance to jamming. Intercepting and decoding well designed secure spread spectrum signals is difficult even for large well equipped intelligence agencies. Decoding some of the commercial spread spectrum data signals can be accomplished by a private individual with the right equipment, but is moderately difficult.

Single channel systems

5. FDMA-FM otherwise known as SCPC-FM.

Single Channel Per Carrier is used to transmit one single nbFM telephone channel between two points. A transponder carries many such FM carriers at one time. Frequencies used are often coordinated by a central station when the call is set up, and may only be used for the duration of the call. This technique is used for communications with remote places that rarely need more than a few circuits at once. Can be relatively easily intercepted by a wide band scanner connected to a very stable block down

(continued on next page)

monitoring phone calls

(continued from previous page)

converter. Easy for private individuals to intercept.

6. FDMA-PCM, otherwise known as SCPC-PCM or SPADE.

This technique is the international standard Intelsat method of establishing telephone connections between places that don't have enough traffic to warrant permanently assigned FDM trunks. Each direction of each telephone call is assigned a channel by the central control station. Stations transmit a PSK keyed carrier on that channel for the duration of the call. Each carrier contains one 8 KHz sampled PCM bitstream along with some error correction and synchronizing bits. As far as I know encryption is not used. The signal can be intercepted by a sophisticated individual but intercepting it requires a rather large dish as the effective radiated power per carrier is very much less than domsat SCPC carriers use. A few domestic satcom SCPC users use PCM, probably with some form of encryption. Hard for a private individual to intercept.

7. FM-FDM-FM (Subcarriers on Video feeds).

As most TVRO owners discover, many of the video feeds contain additional subcarriers that carry unrelated or tangentially related material. Included among these are cue and coordination channels that may occasionally carry telephone-like conversations. There are no regular telephone circuits on video subcarriers however. These subcarriers are trivially easy to intercept as most TVRO's have tunable audio demodulation.

On FM-FDM-SSB

All it takes to recover FM-FDM-SSB signals is a suitable wideband FM receiver connected to a stable general coverage SSB receiver that tunes the frequency range used for the baseband. TVRO receivers have the correct bandwidth for many such signals and often incorporate provisions for IF filters that can be used to better adapt the receiver to the narrow band signals found on some transponders. And modern general coverage SSB receivers and transceiver receiver sections with synthesized tuning, digital frequency display, and narrow IF filters are well suited to recovering the audio on a particular channel.

Listening to FM-FDM-SSB signals can be accomplished by tuning the TVRO receiver to

either a satellite transponder carrying an FM-FDM-SSB signal (this may involve restricting the IF bandwidth with a filter as some transponders carry more than one FDM-FM signal), or pointing the antenna at a nearby terrestrial microwave transmitter and tuning the receiver for maximum signal.

Once the FDM-FM signal has been tuned in, the single sideband receiver can be used to search the baseband (typically .3 Mhz to 6 or 8 Mhz) for telephone conversations, data transmissions, and other private line circuits. Individual channels will appear as USB or LSB signals at precise 4 KHz intervals. In fact, the whole baseband is organized into 12 channel groups, 60 channel supergroups, and 600 channel mastergroups according to a standard frequency plan (the AT&T plan as usual is different from the CCITT one used internationally).

"Nothing in the Electronic Communications Privacy Act of 1986 requires carriers to increase the security of radio or satellite links."

Most channels have completely suppressed carriers, although certain channels will seem to have a carrier in them (but slightly off frequency) which is something called a pilot tone, used to monitor circuit continuity and control overall gain. Depending on how archaic the telephone trunk equipment is on a particular trunk, it may have a 2600 hz SF signalling tone in it when it is idle which is dropped when the channel is in use for a call. Trunks which use SF signalling also often use MFKP (multi-frequency key-pulsing—the famous blue box version of tone dialing) to pass telephone numbers on to the destination switch. More modern trunks use CCIS (common control interoffice signalling) which is a packet network replacement for the earlier and less secure in band signalling that uses separate signalling channels to carry all the signalling for all the trunks in a trunk route.

Obviously, a single signal usually carries only half a telephone conversation so it is necessary to use two receivers and TVRO's to pick up both

with a TVRO

sides of the call clearly. Receiving both sides of a terrestrial circuit requires a suitable location where both directions of transmission can be picked up, which usually means a site in line with the microwave path. Sometimes both directions of transmission from a single repeater site can be monitored by a very nearby (less than a couple of miles) receiver. Many telephone trunks have low enough echo return loss so that both parties can be heard even when monitoring only one direction of transmission, so it is quite possible to listen to both sides of some conversations with only one receiver. Both sides of a satellite FDM circuit can usually be found on the same bird but are sometimes not, and sometimes not even on FDM satcom at all.

In general, particularly on terrestrial signals, all the channels in a 12 channel group originate and terminate at the same place. The groups and supergroups that make up a mastergroup however often originate from several different places. Demodulation to baseband audio is generally done as few times as possible on a trunk or private line circuit that connects two places, the 12 channels of its group are shifted to various frequencies within the baseband of the different satellite, microwave, or coaxial cable FDM signals that carry it to its destination, but at least with older multiplexing equipment the granularity of routing resolution is usually a group (occasionally half a group), and all 12 of the channels in a group usually end up demodulated to audio at the same place.

Channels within a group are assigned to various purposes. Some may carry telephone trunks, some may carry private line data, some may carry private trunks that belong to large companies, and a certain percentage are reserved for use as spares. It has long been telephone company practice to route the telephone trunks between two switching centers over several different paths to supply redundancy in the event one path fails (and also to make it harder to intercept a particular call between the two switches). This means that any given FDM group may contain trunks from several different trunk groups rather than containing all the trunks from, for example, Chicago to West Bend.

On PSK TDM

The most secure technique in commercial service, and probably the technique that will

predominate on satellite links in the future, is TDM-PCM (time division multiplexed pulse code modulation) either phase shift keying (usually QPSK) a continuous carrier on a transponder that may have several such carriers on it (FDMA—frequency division multiple access) or keying a single carrier that occupies the whole transponder in bursts precisely timed so as to not overlap other carriers from other stations that it shares a transponder with (TDMA—time division multiple access).

Telephone traffic on TDM-PCM links is sampled 8000 times a second and converted into 8 bit binary values (in a sort of floating point format called A-law or μ -law companding that greatly expands the dynamic range from softest to loudest that the channel will handle). (There are other digitizing standards used on satellite phone links but the standard T carrier—D channel bank is widely used.) Some number of these channels (often 24) are combined into a high speed serial bit stream (often 1.554 mb/s) by sending one sample from each channel in serial form as a string of 8 bits followed by a sample from the next channel and so forth. Sometimes this composite bit stream or the bit stream from individual is encrypted with a DES chip. Error correction and framing bits and sometimes special control channel bits are added. This digital bit stream is then scrambled (so it has more predictable transition statistics and little or no DC component) by a linear feedback shift register sequence. The resultant bit stream is used to PSK modulate a carrier which is uplinked to the satellite.

Receiving these FDMA-PSK-TDM-PCM digital transmissions requires complex RF modems, a large enough dish to get an acceptable signal to noise ratio (and BER), and often requires knowledge of DES encryption keys used (unless you are a major intelligence agency and can break DES). While some such transmissions that aren't encrypted could be intercepted by a sophisticated individual, particularly one who had access to the RF modem and multiplexing hardware used by the subscribers, the required expertise is orders of magnitude greater than that required to intercept FM-FMD-SSB signals and the equipment required is specialized and not widely available. (Decoders for TDM-PCM bit streams could be

(continued on next page)

monitoring with TVRO

(continued from previous page)

built by a skilled person from available chips relatively easily, but the PSK high speed RF modem technology used would not be easy for even a skilled person to duplicate without substantial resources.) Presumably few if any casual listeners intercept TDM-PCM radio circuits; the only listeners to such transmissions are the intelligence agencies and perhaps industrial spies who can afford to buy the necessary hardware to listen to their competitors' private circuits. And more and more users of such links are encrypting them with DES (which is relatively easy as the information is already in a digital format).

TDMA-PSK-TDM-PCM signals are much more complex than most FDMA-PSK-TDM-PCM signals. This is natural since all traffic is transmitted by having each station on the network transmit a burst of very high speed (tens of mb/s) data in an assigned time slot round robin fashion. Included in the burst is all of the traffic that station has with every other station on the network. Every other station monitors all the bursts from stations it is in communication with and picks out the channels that correspond to its incoming traffic. In many such systems, burst lengths and time slots are dynamically assigned by a master ground station computer as calls are

set up and terminated. Each station is capable of receiving and decoding the bursts transmitted by every other station it talks to, so if the channels are not encrypted it could monitor much of or all the traffic going through the transponder.

The burst formats are complex and contain error correction, status and control channels, call setup channels, and so forth. And the bursts are scrambled just as in the continuous carrier TDM case. Intercepting and demodulating such a signal would be a major task and is probably something that has only been done (by intelligence agencies) by using perverted versions of the ground station hardware and firmware used by the system. In addition to the complexity of the task of sorting out the digital information and finding the right time slot from the right burst to retrieve the channel of interest, the very high speed fast lockon RF modems used to demodulate the bursts are themselves non-trivial devices. I suspect that even perverting the firmware in a legitimate ground terminal is complex enough so that no private individual could easily accomplish it without access to a lot of detailed non-published information (such as source of the firmware and precise details of the protocol and burst formats).

(continued from page 3)

We're happy to announce our affiliation with another computer bulletin board system, our third to date. It's located in Columbus, Nebraska and can be reached 24 hours a day at 402-564-4518. We expect to have more 2600 bulletin boards on line by the summer.

We've also been getting a lot of positive press response in the past couple of months, including a spot on a most incredible television program, Network 7 on England's Channel 4. This program ought to be seen by every reporter in this country who wants to do a story on computer hacking. Instead of looking at the "problem" of hackers and what they could be doing to you in the same way we've seen hundreds of times already,

the producers of this program looked at the positive aspects—the adventure, imagination, and intelligence involved. It wasn't just that they gave hackers a positive image—they used their brains and created a different way of viewing a topic. That's something we can all use a bit more of. Our thanks to John Drake for making this possible.

It's possible the press is finally growing up and realizing that hacking involves so much more than electronic bandits. It's a symbol of our times and one of the hopes of the future. If that sounds crazy to you, wander through our pages and it may start to make sense.

VM/CMS CORRECTIONS

by VM Guru

As *2600* has published information about various aspects of UNIX and its cousins, my attitude has been more or less ho-hum as I had little interest in these systems. When I saw on the back cover of the November 1987 and December 1987 issues that there was some material on VM/CMS, my interest perked up. That's a system that I know and love, as I have been working as a VM system programmer for many years. The article makes it obvious to me that "Lex Luthor" et al has only a superficial knowledge of VM/CMS, I would like to take this opportunity to fill in some of the gaps and give *2600's* readers a more complete picture of VM.

Comments on Part 1

A few general points to start:

- There are two types of VM systems. The first is (usually) fairly small, typically on an IBM 4331, 4341, 4361, or 4381. They are generally unmodified and tend to use the IBM default names for system userids and often passwords. Unless you work there, cracking these systems will be difficult because they usually have no data connections to the outside world.

- The other general class of VM system is fairly large, running on a CPU such as a 3081 or 3090. These systems are often modified, both to provide function and security. Some of these mods are described below. Many of these mods are passed around at conferences, workshops, or by a conferencing (BBS) system (which will remain nameless).

- The VM system lends itself to modification because most of the source code is distributed with it. For a long time, IBM treated VM as an orphan stepchild and tried to bury it. The users wouldn't let them, and IBM finally recognized it as a going system. VM has now passed through eleven releases, and the twelfth has been announced.

- VM (or CP, the two terms are often used interchangeably) is not an "operating system" in the usual sense of the term. You can't run "jobs" (processes) under it. Rather, you run operating systems under it and each user runs an operating system. Each logged on user gets a "virtual machine" to run his operating system in. Each virtual machine has a CPU, memory (storage), disks, tapes, and unit record (card or printer)

devices. Some of these correspond to real devices, and others are virtual. A virtual disk can be represented by a small portion of a real disk. Unit record is usually "spooled" to/from disk. Most systems these days have no real card equipment, and the virtual card equipment allows data to be passed between users as "card images" (80 byte records). All functions that would be buttons, dials, or lights on a real machine are represented by query or set commands to CP in a virtual machine.

- CMS is a single user interactive operating system that is tailored to run very well under VM.

- Other operating systems that are often run under VM are batch systems such as MVS, DOS/VSE, or VS1. These can run both batch or interactive systems such as TSO, CICS, ICCF, or others. (See the discussion of DIAL below.) A second copy of VM can run under VM, and this is often used to test modifications and new releases. Basically, anything that can be run on the real hardware can be run under VM in a virtual machine.

- VM natively supports three types of terminal. These are 3270 display (CRT, video) terminals (in many flavors), 2741/3767 (typewriter-like terminals), and ASCII terminals such as the IBM 3101, TTY's, and ASCII CRT's (such as the VT-100) in line mode. A PC that emulates one of these can also be used. To support ASCII CRT's in full screen, a protocol converter is needed. Both hardware and software versions of protocol converters are available. These make the ASCII CRT look to the VM system as if it were a 3270 terminal. Various escape sequences are used to simulate 3270 functions that the ASCII CRT may not have.

To cover Lex Luthor's article point by point: (When I refer to commands, I will use the IBM standard names. Some installations have modified these names.)

- While it was late in coming, VM has had online help for some time. It's slow, it's clumsy, but it's there. Enter "HELP HELP" to get started.

- While the system is somewhat cumbersome, that's mainly because of the wealth of functions available. If you found it hard to learn, then either you didn't have the manuals that are needed, or you had a poor teacher (or

(continued on next page)

VM/CMS CORRECTIONS

(continued from previous page)

both). VM/CMS is just too big to pick up on your own without some guidance.

- I won't comment on the acronym list except to say that it only scratches the surface.

- The "." prompt is only seen logging on via an ASCII terminal, and is a "go ahead" signal. Most other terminals supported by VM can have their keyboards locked by VM. It can be turned off, and a common modification is to replace it, sometimes with a "bell" character.

- The "VM/370 ONLINE" prompt (followed by the list of acceptable commands in newer versions of VM) is the only IBM-supplied connection prompt. It is often replaced by the system or company name. The other connection responses Lex mentions are from front end processors or networks, and precede the actual connection to the VM system.

- While some other IBM systems do require it, it is *not* correct that userids (or passwords or even commands) in VM/CMS have to start with a letter. An all numeric userid or password is valid (but not commonly used), and the "national" characters "\$", "@", and "#" can also be used. Certain characters are used as editing characters. A pound sign ("#") is a logical line end. It can be used to separate multiple commands or data lines entered at one time on one terminal line. An at sign ("@") is a character-delete character. One or more at signs will delete the same number of previously entered characters, perhaps saving the retyping of a long line. For example, if "aaa@@bc" is entered, it would be interpreted as "abc". For total foul-ups, the cent sign will tell VM to ignore everything to the left of it so you can start again. For ASCII terminals that don't have a cent sign, the VM system uses the left square bracket instead. And what do you do if you want to enter one of these characters as data? That's where the fourth one comes into play. If any of them is preceded by a double quote, the character pair will be treated as a single data character; i.e. "# will be treated as a pound sign without being used as an editing character. All of these can be changed to whatever character (not A-Z or 0-9) you wish or they can be turned off. The character-delete is often set to a backspace character if the terminal has that key (most IBM typewriter terminals don't). The "QUERY TERMINAL" command will display the current settings of these characters

as well as show other information.

- Some VM security packages use a password up to 24 characters long. (More on them later.)

- Lex is correct that the only currently used IBM logon qualifier is "NOIPL", but others such as terminal type or altering the virtual storage size are common mods. An obsolete qualifier of "MASK" used to be used to tell VM to type a mask (overprinted lines of "*", "H", and "S") so that when you typed your password over the mask, it could not be read. MASK is now the default, and will be ignored if entered. Most larger installations use the password suppression option.

- A common mod is that if an invalid userid is entered, prompt for the password anyway, and then reject the attempt no matter what password is entered.

- Messages warning of exceeding the invalid password threshold are sent to the system operator and/or the system security administrator. It is also recorded in the system's journal (accounting) file.

- The reason that "BONEHEAD" (to use Lex's example) is "not valid before logon" is that because of the extensibility of VM/CMS, BONEHEAD could very possibly be a valid command, either local to one user, a group of users, or systemwide.

- In a large system, it will be very unlikely to find any passwords that are the same as the userid, or are still at the IBM-supplied defaults. Many security packages force a user to change his password at regular intervals.

- Just because you see a userid, don't make any assumptions about what it does. For example, a large American university has a userid up and running which is the name of the security package they use. It's a dummy, and the security package actually runs under a very innocent userid.

- The DIAL command is used when the operating system running in a virtual machine is a multi-user system such as TSO, CICS, ICCF, another copy of VM, etc. DIAL establishes a connection between a real terminal, and a virtual port defined for the multi-user system. Security in this case is the responsibility of the multi-user system, except that an available mod requires a password to do a DIAL. Other available mods

(continued on page 12)



Bell of Pennsylvania

A Bell Atlantic Company

To Our Valued Customer:

● **Here Is Your New Directory**

● **If Your New Directory
Is Damaged, Call
1-800-555-5000**

● **We Will Replace It
Free Of Charge**

Warning: May Be Hazardous To Children

YELLOW PAGES

BELL ATLANTIC CUSTOMERS RECENTLY RECEIVED THIS BLURB ON A PLASTIC BAG CONTAINING THEIR NEW YELLOW PAGES. WE'RE GLAD SOMEONE'S FINALLY REALIZED THE DANGERS THAT YELLOW PAGES CAN POSE TO KIDS.

VM/CMS

(continued from page 10)

force specific real terminals to connect only to specific ports (or port groups).

- A message to the operator as Lex suggests will bring the security administrator down on you in many systems. In most VM systems, the operator could not give you the password, as he has no access to the directory. In many larger systems, the OPERATOR id (which doesn't have to be called OPERATOR) is disconnected and is running a program called PROP (PRogrammed OPerator). PROP will respond to routine messages, and route others to "logical operators" such as disk operator, tape operator, or security admin.

- On the monitoring and recording of invalid and privileged commands, this is available as part of standard VM. Because the VM monitor function has high overhead, it is (usually) not done on a regular basis, but is turned on for sample periods or when a problem is suspected. There are mods and packages available which will record all valid and invalid command usage and the resources that the command consumes with minimal overhead.

- The QUERY NAMES command could (on a large system) show several hundred logged on users. An available mod limits it to users in the same group as yours, either by using the account code or a portion of the userid. The order shown has no connection with the order that users logged on. It is simply following an internal chained list of all users, and it stops when it gets back to you. This list has three parts. Above the "VSM—....." line, users are logged in with locally attached (or in some cases, TYMNET or its ilk) terminals. The three-digit (four in some larger systems) hex number following the userid is the hex hardware address of the terminal. If your userid is shown in this section, your userid will be the last one in the list. The "VSM—....." line identifies the "VTAM SERVICE MACHINE". This is the link into an IBM SNA (System Network Architecture) network. Users listed below there are connected to VM through a VTAM network which could span many processors and many miles. The name following the userid is the LU (Logical Unit) name of the terminal, which is used as a network address. These two portions of the list will be absent if the VM system is not connected to an SNA network. The last portion will be missing if the system is

connected to an SNA network, but no users are currently logged on from it.

- On a QUERY USERS response, the number of USERS and NET will be the number of users in the first and last parts respectively of the QUERY NAMES list. The DIALED number is the number of users connected to multi-user systems.

- One type of multi-user system you could DIAL to is called a "session manager". This allows you to create several "Logical Terminals" and log each one onto a different userid (or DIAL to a different system). These logical terminals will show in a QUERY NAMES list as "Lxxx" where xxx is a three-digit hex number which can range from 000 to FFF. For logical terminals, the program accepts the data that is to be displayed on the terminal, and simulates entering data on the keyboard. In many systems, creation of a logical device is made a privileged function to reduce the likelihood of a hacker making a "trojan horse". The session manager allows you to switch between your various sessions, with the active one showing on the real terminal. Session managers are usually used with video terminals (CRT's).

"While the system is somewhat cumbersome, that's mainly because of the wealth of functions available."

- A disconnected user (shown on a QUERY NAMES as "DSC") can remain logged on indefinitely. It will only be logged off by the system after 15 minutes (modifiable) if it tries to read from the terminal it doesn't have. DSC users are usually service machines such as security, accounting, utility, database, and other functions. Some large systems have 50 to 100 of them running.

- "Userid NETLOG" is located on your logon, and contains information on files that you SEND to others, and that you RECEIVE from others. It is logged when *you* receive the file, not when *they* send it to you. The "USERID" in the name will be your userid, not the userid you sent the file to.

CORRECTIONS

Comments on Part 2

The second part of the article on VM/CMS is just as full of errors and misconceptions as the first. As in part one, I will address Lex's article point by point with expansions and asides as appropriate.

- Local commands: This is one of the strong points of VM/CMS, that is, it can be extended with local commands. These can be in any of the three flavors of exec languages (interpreted command processors) or any compiled language. To execute it, just have it on any disk that is available to you (private, public) and call it by name. Getting back to "WHOIS", I am surprised that VMUTIL is shown as a statistical machine. That name is (usually) used for an IBM program of the same name that is timer and event driven for a variety of purposes. The WHOIS output may be a red herring.

- As an aside, CMS has a complex scheme to locate a command. When you enter a line at the terminal, CMS takes the first blank delimited word, uppercases it, and truncates it to eight characters if it's longer. Then it goes through the following search. If any step of the search finds the command, it stops there. If they all fail, you get an error message.

1. Search for an EXEC with a filetype of EXEC that is resident in storage. If this search succeeds, the proper EXEC interpreter (there are three exec languages available) is called to interpret the file.

2. Search for a file with filetype of EXEC on any currently accessed disk. CMS uses the "standard search order" (filemodes A-Z). The table of active (open) files is searched first. An open file may be used ahead of a file that resides on a disk earlier in the search order.

3. Search for a valid synonym (system and user supplied synonym lists) for a storage resident EXEC.

4. Search for a valid synonym for a disk resident EXEC.

5. Search for a nucleus extension command. These are storage resident commands that can replace or front end standard or user commands, or can be unrelated to standard commands and just kept residents to reduce overhead of loading them multiple times. Some commands make themselves into nucleus extensions the first time they are called so that subsequent calls will have lower overhead.

6. Search for a command previously loaded into the transient area. (An 8k buffer in the nucleus.)

7. Search for a nucleus resident command.

8. Search for a file with filetype MODULE on any currently accessed disk. If found, the MODULE (executable code) is loaded and branched to.

9. Search for a valid abbreviation or truncation of a nucleus extension. Most CMS (system supplied) commands can be abbreviated to the minimum length that is not ambiguous.

10. Search for a valid abbreviation or truncation of a command in the transient area.

11. Search for a valid abbreviation or truncation of a command resident in the nucleus.

12. Search for a valid abbreviation or truncation of any other CMS command.

13. Search for a CP command.

14. Search for a valid abbreviation or truncation of a CP command.

- Password changing at many installations is under control of a directory maintenance or security system. In many cases, the system forces users to change their passwords at regular intervals, and some are smart enough to remember the last n passwords and will prevent you from re-using the same password over again for a while.

- Re privileged commands: The sysprog can determine the priv classes of a logged on user (there are 32 possible classes (A-Z and 0-5), only seven of which are used in standard IBM code) by examining real storage in the CPU. It takes class C or E to examine real storage. VM in concert with various security or monitoring packages can record command usage, both failed and successful. In VM proper, this monitor function is high overhead and is (usually) used only for sample intervals or when a problem is suspected. Other packages are available that would monitor commands with minimal overhead.

- In the Q SEARCH output, the 19E (Y) disk is usually used to store any commands that are local to this system. The 190 (S) disk is usually the IBM supplied code. The Y/S means that if a request to get something from the S disk is issued, and it is not there, the Y disk will be searched as an extension of the S disk. The volume name (also known as the volid or volser)

(continued on next page)

VM/CMS CORRECTIONS

(continued from previous page)

is not processed by CMS.

- The filemode letter is the same as the disk the file resides on is accessed as. If you release (logical detach) a disk and access it as a different letter, LISTFILE will then show the same files with the new letter. If you add the option "LABEL" to the LISTFILE, a lot more information for each file will be shown. This includes the file size, record format (fixed or variable), record length, last updated date-time, etc.

- In the list of filetypes, there are some errors. System help files have a filetype of "HELPPxxx" where "xxx" is a subpart of the system such as "CMS", "CP", "REXX", etc. These help files are (usually) found on the 19D disk. Under the LANGUAGES item, programs written in rexx would normally have a filetype of EXEC. LISTING files can contain anything. Their distinguishing characteristic is that they usually contain printer carriage control characters as the first byte of each line. MODULE files can be any executable program, system or local. TEXT is usually used for compiler output. XEDIT is the filetype used for XEDIT (the system editor) macros, which are usually written in rexx or exec2. The editor can create a file of any filetype. Lex's description of the filemode numbers is essentially correct. There are many ways to break the filemode zero security so it should not be relied upon.

- Re Passwords: The "PASS=" keyword is optional. If used, be sure to put a space after it. (I am not sure if that was a typo or a Lex error.) There is no VM restriction to using the same password for login and disks, and all three disk passwords can be the same. Some security systems forbid this, and it is not a good idea in any case.

- Re the Q DASD command shown. If you have gotten onto a privileged id, this will show the real dasd that the entire system has. In this case, a "Q Virtual DASD" request will show your own disks. In the display as shown, "SYSRES" is the volser of the real disk that these minidisks are a part of. A partial listing of the real disks might look like this:

```
DASD 130 CP OWNED VMIPOE 0044
DASD 154 CP SYSTEM SYSWK1 0001
DASD 249 ATTACH TO VSEIPO 246
```

What this listing shows is that VMIPOE on real address 130, is "OWNED" by CP (i.e., it

contains one or more system data areas), and the currently logged on users have 44 minidisks on this pack. This can be 44 users all with the same minidisk, 44 different minidisks, or some combination. SYSWK1 is on 154, has no system data areas, and at the moment is in use by one user with one minidisk. Real address 249 is attached (dedicated) to user VSEIPO as his virtual address 246.

- There is nothing in the DIRMAINT package that requires its userid to be DIRMAINT. It often is because that is the default name unless the sysprog changes it during installation. The DIRM LINK command can only be done if you know the password for the link mode you are asking for. The disk's owner is notified when you get a link in this way. Many DIRMAINT commands can be locally disabled as an option during installation. Enter DIRM ? for a list of commands, or DIRM ? command for details on a given command.

- The system directory can have any name but usually has a filetype of DIRECT. Another common name is VMUSERS. Where Lex shows a "typical" entry in USER DIRECT, ignore the lines starting with VMU01.... These are sequence numbers in columns 73-80 of the file which have been broken into 2 lines for some reason. Most likely you or the system has defaulted the line length of the terminal to 72. The two storage sizes (1M and 3M) are the default size and the maximum you can ask for (with the DEFine STORage...command). The IPL statement says to automatically IPL (Initial Program Load) the system named CMS at logon. The CONSOLE line defines that the user's logon terminal is to look like a 3215 (IBM typewriter terminal) at address 00D. 009 or 01F are more commonly used console addresses. The three SPOOL statements define the virtual card reader, card punch, and line printer available to this user. The three LINK statements get access to the CMS system disks.

In conclusion, I hope that I have been able to correct most of the errors and misconceptions that Lex has given you. As he did, I have omitted several things that would be dangerous for a hacker to know about VM internals. There were a lot of holes in a VM/CMS system, but most of these have been plugged by IBM or users. I hope that both Lex's articles and mine have been of interest to the readership of 2600.

An Interpretation

The following article is one view of computer hackers. We'd like to say right up front that it is not ours and in fact we take exception to a good many of the facts presented. We would be most interested in hearing what the hackers of the world have to say regarding this perception of them. Please send us your feedback.

by Captain Zap

The ongoing wave of computer crime that is being reported in the media around the world shows the ease of computer system break-ins that are becoming more and more widespread. Both the technology and the society have changed since the birth of the first computer and the growth of the computer has come to the average household in the U.S.

The speed has increased while the size has shrunk. One simply has to compare the Apple or IBM personal computer to ENIAC, the first computer. ENIAC was very large and needed a small electrical sub-station to operate while the personal computer today runs on batteries or household electric. The memory in ENIAC was just about 2k compared to today's personal computers which commonly have 16 Megabytes of RAM.

All of this computing power is now in the hands of everyday persons and the equipment can be carried to anywhere in the world. In addition these people can gain access to the computer center of any major and a large number of minor computer sites. How? Through the phone lines around the world and the ability of such a vast global network to interface almost anywhere on the face of the planet. Simply put the phone and the computer are now one and the use of dial-up ports to the computer is becoming standard operating procedure. The reasons are due to the desire for distributed databases and the need for all of the information to flow over the phone networks around the world. We will now look at the issue of information flow over the phone network and how easy it is for someone to gain access to any part of the transmission.

Telecommunications and Fraud

The beginning of the formal underground phone network started in 1971 with the formation of the newsletter entitled "YIPL" or

Youth International Party Line. This newsletter was structured with information on how the phone company equipment would work and ways to defeat it. This was also seen as a protest against the Vietnam war and the federal tax that was placed on phone service to help pay for the war.

The idea was to be able to place calls to others without paying any form of toll charge. This one form of toll fraud was done with the use of homemade electronic gear known to this day as the "blue box". The "box" was able to simulate the signals of the phone company switches and it could place calls as if one had the same controls as a regular AT&T operator.

Calls were placed over toll-free trunks such as 800 numbers. The phone company, seeing the problem, placed a tone detector on trunks looking for the distinct tone frequency of 2600 Hertz. (This tone is the signaling frequency for the long-distance trunks to disconnect but the blue box could still maintain a hold on the trunk and place calls from remote locations.)

One other interesting aspect should be mentioned—the use of a whistle that was found in the boxes of "Captain Crunch" cereal. The name "Captain Crunch" was used by the earliest phone phreak known to the phone system security force. His real name is John Draper and he was the first person who used this whistle from the cereal boxes and discovered that the toy would produce the exact same tone (2600 Hertz) that the phone system produced for the seizure of the trunk lines needed to make long-distance phone calls.

Other "boxes" also exist. Here is a brief list:

Blue: produces all (SF) single frequency tones and (DTMF) dual tone multi-frequency. Able to dial without incurring toll charges.

Red: able to produce coin identification tones that correspond to coins placed in a payphone (nickel, dime, or quarter).

Green: coin return. This allows the caller to return coins instead of the coins dropping into the coinbox of the payphone.

Silver: able to simulate the DTMF and have the availability of generating 1633 Hz. Tones are used on the Autovon voice network (the military phone system).

Black: does not allow the connection of billing

of Computer Hacking

circuits to call. Must be used on called party's line. This is only usable on older switches such as step by step or #2 or #5 Crossbar.

Clear: allows for calls to be placed from the new private payphones that block the phone's microphone until a coin is inserted. But by using an impedance tap type of device the speech of the caller can be electronically placed in the earpiece and the conversation can proceed normally.

Cheese: allows for a call to be placed to one location and then transferred to another location on a different line than the original number called. Used to hide actual location of the caller from traces by separating and isolating the call from the other line.

There are combinations to these boxes. They can be red-blue or red-green or silver-red-blue.

But one of the simplest ways to defeat the phone system would be to use a portable tape recorder. This would allow for the tones to be played into the mouthpiece or to use an induction coupler to enter the tones. This way there is no illegal equipment to be found and the phone phreak can do his work.

"Computing power is now in the hands of everyday persons and the equipment can be carried to anywhere in the world."

Other methods of phone fraud are now taking place due to the use of other long distance carrier networks. Carriers such as MCI and Sprint have had toll fraud problems for years and now are starting to compare notes about toll fraud and other pertinent information. The carriers have recently formed a group that pools information about suspected code abuse. Such information includes phone numbers dialed, called party name and address, suspected or known toll abusers, and the new problem of multi-carrier abuse.

Most of the known abuse is being directed from the hacker bulletin boards that post port numbers and access codes. Other incidents include employee use after hours or just plain fraud by using another person's code.

We will first discuss the problem of multi-carrier abuse or "weaving" through the different networks. This form of toll abuse gets its name due to the way that calls are placed to the target phone.

In the U.S., there are five major long-distance telecommunications carriers: AT&T, US Sprint, MCI, Allnet, and RCI.

If a caller wanted to hide in the different networks, he could start by dialing a local PBX (Private Branch Exchange) and use the PBX as the first point of contact to place the call. Most major PBX's today have the ability to allow outsiders to gain access to the local telephone line through a switch in the PBX.

This switch gives the local dial tone and allows a call to be placed to the first local access port of one of the common carriers. The local port answers and places a carrier or system dial tone across the line and the caller inputs the access code, area code, and number to the next target switch.

The number input is the number of a target switch in another city and allows for the caller to hide in the network of Bell and the first carrier. The second targeted switch then answers and gives a system dial tone and the process is repeated.

This progression will continue until the final target phone line is reached. Such tactics can confuse even the best telephone company attempts to trace a call. So the final product of the call is that the caller could be coming from any major port on any of the carriers. Plus the added problem of being on all carriers at the same time with the different interconnections allows for some very interesting complications to occur.

Such access to the switch is very easy as many persons use these common carriers to make long-distance calls. With the vast amount of persons who use such services, the ability to find working accounting codes is still very easy! Such codes can be found by the use of a modified "Wargames" dialer program. This particular program will call the local port of the common carrier and just like its cousin the port scanner, will scan the common carrier port with the ability to generate touch-tones and "hack" out a working code that can be used for that switch.

An example of a simple "Wargames" program

(continued on next page)

(continued from previous page)

is listed. This program was written for use with an Apple II+ and a Hayes Micromodem.

The operation of the program is very slow but other faster versions of this are available to the system hacker. Other programs have been written for use by the Hayes Smartmodem and the Prometheus ProModem 1200A.

(See WARGAMES listing on page 20)

It should be noted that some of the common carriers have changed the programming of their switches to only accept valid codes for the local area—that is, not to accept any other code that might work in other parts of the country. Traveling callers must call a special number and insert an additional 4-digit code after the regular authorization code.

Hacker Communications and Bulletin Boards

Some of the ways that the hackers communicate is through the use of conference calls and the underground bulletin boards. Such methods of message traffic go without charge and are able to be done by the vast majority of the hackers. The hackers have the ability to place up to 30 calls to any place in the world and join all of these calls together.

Most of the calls are placed to pass information over to other hackers that can work on a problem and compare results and plan for more tactical attacks to the target system.

The logic behind the thought is that the ability of one person to attack a system is multiplied tenfold by the others working on the same system.

Such attacks have been placed on varied computer and communications systems by the hackers. One such incident took place in Los Angeles, with phone phreaks and hackers attacking the Bell System master control computers and trying to turn off all the phones in the city with the exception of the emergency circuits. This attack was for the most part successful resulting in the loss of phone service for thousands, but not complete in its goal.

But this writer's opinion about the attack is that it was very successful showing the ability of certain persons who were able to shut down some of the phone service in the city. If such actions can be performed by persons who do not have inside information or access to the facilities, then it is a very real situation. Such attacks can be

The Threat of

placed to a series of phone lines or just one. Other attacks have involved the reprogramming of Bell System switches, changing the destination of 800 toll-free calls to other locations, or ringing a vast number of phones at the same time.

The phone/computer underground is still growing with the vast amount of personal computers coming into the hands of many different persons who now have a large amount of computing power at their fingertips.

Bulletin Board Systems

Bulletin boards are, as they sound, a place where persons can place information or requests for information. But in the world of the hackers, the bulletin boards are a way to pass information via computer to other hackers. These boards are set up by individuals in their homes and the users of the board call a phone number that is attached to a modem and the host computer. A bulletin board is nothing more than a place to swap information.

Such information like dial-up port numbers, logons, and passwords are common information available to the main hacker population. Other more secret information is passed in confidential messages to each other and through the use of sub-sections of the board where only a select few are able to enter.

The bulletin boards contain a wealth of information if one can gain access to them. One reason that the boards are difficult to enter is because of their security. A good rule to remember is that the hacker bulletin boards have far better security than most large computer systems, and that the hackers check out each user for their real identity. A series of checks is done that include the place of employment, the phone number and the owner of that number, driver's license, health records, and the like. Other security checks require that a prospective user be recommended by another user to gain access, and then the new user is granted a lower status than most users until he proves his worth in the hacker world. The chance of a law enforcement person gaining access is thereby greatly reduced. Other aspects of the security of the boards is that some of them have a clause at the sign-on that states that the board is not responsible for the information posted and that any information placed on the board is for informational purposes only and that the person

Computer Hackers

who is logging onto the system is not a member of any law enforcement agency in any way, shape, or form.

One of the methods used by the hackers to keep control and order in the hacker community is known as Tele-Trial. Tele-Trial is a court that is convened by the hackers to listen to complaints, set laws, and hand down decrees upon suspects. Such decrees can include not granting access to the boards or having someone executed electronically. Such actions have come to the public's attention with the Tele-Trial of *Newsweek* reporter Richard Sandza. The story with Mr. Sandza is that he wrote an article about the hacker community and the hackers did not approve of the story, so Mr. Sandza had his credit card information posted on a number of bulletin boards and numerous articles delivered to his home.

Other interesting parts of this story include the distribution of his private non-published phone number and a number of death threats. Mr. Sandza then wrote an article entitled "Revenge of the Hackers" and was bombarded with another wave of abuse from the hackers. This writer's opinion is that it is better to make an ally with the hacker rather than to antagonize him, as he can perform your destruction in a matter of seconds and such destruction can happen at any time. And remember, the hacker can be the best prevention for computer security sickness and that a reformed hacker can make for the best data processing security person.

In general, most of the computer bulletin boards are nothing more than a place where persons of general interest are allowed to communicate their ideas and comments about hobbies, art, science, cars, ham radio and electronics, and of course the major reason this article has been prepared—the computer/phone underground. The boards in general have been a major problem in the control of information due to the use of the boards by what some may call "information junkies".

But the problem of the "information junkies" is one that is spanning the computer arena with all types of persons using this form of high speed communication. And one of the major contributing factors involving the computer abuse is the non-education of the users in ethics.

But the problem is twofold: the user must be

held accountable for his actions and the owners must secure their machines with a reasonable amount of security.

Part of the problem with the owners and of course the transmission facilities is that the carriers do not take responsibility for the security of the transmission, only that the transmission will get to the intended destination. Add to that the cost of point-to-point encryption and you get very high costs both in the equipment and in the maintenance of the system.

"The boards are considered a major nuisance to the phone companies."

The bulletin boards contain a vast amount of information at the fingertips of thousands of persons at any time. Some of the boards have the ability to have multiple users on them at one time. And the boards that we will concern ourselves with, the underground or clandestine boards, are the toughest to crack. Information on these systems can range anywhere from how to make free telephone calls to the formulation of crude plastic explosives to a person's credit and personal information. Mostly the boards are a place where the study of telecommunications and computers is placed above all other things. The hackers call it nothing more than "electronic geography". They have nothing more than a good sense of curiosity and they want to learn. So they go exploring and find things that most would consider to be trivial. Information found has been well documented and proven to be embarrassing to the owners. The government has therefore given both the Secret Service and the FBI the job of investigating all computer crimes. This includes the investigation of the underground bulletin boards.

The boards are considered a major nuisance to the phone companies, but are only considered a small threat to the computer owner. But they still produce good copy for the morning paper and evening news. The general public thinks that the hackers are wonder kids able to launch a nuclear missile in any direction who can invade any

(continued on next page)

The Hacker Threat

(continued from previous page)

computer system out there. They hear that a computer that belongs to the U.S. government in a nuclear research facility has been "tapped" by the hackers, or that there is a possibility of the hackers controlling satellites and moving them out of their assigned orbits. Granted, they did not move the bird, but they did gain access to the rotation control for the satellite.

And it was stated that the information needed to do such things was found on an underground bulletin board. That might be true, but information that is far more valuable to people on earth is being posted on the boards. And this information comes from the trash can or from insiders who have become disgruntled or just from plain old research—looking for publicly available sources. Some of these public sources constitute users' manuals and system documentation.

Another interesting fact about the boards is

that they contain a group of sub-sections that include subjects on telecommunications, software piracy, and cracking of software protection systems, computer systems overviews and how different systems work, and ways around the system security features. Some bulletin boards also contain page after page of dial-ups to major computers around the country. These include all of the Fortune 500 companies and a large amount of military systems. So to the persons who state that the bulletin boards are not a problem, I believe that they have not been on any of the major underground boards and therefore should not make such rash statements.

As to the overall damage that a bulletin board can cause, the final cost has yet to be determined. The boards allow for the transmission of information to a large group of persons. What the person who gets this information does with it is another story.

```
1  REM "WARGAMES DIALER PROGRAM" FILE MUST BE OPEN FIRST
5  INPUT "NUMBER TO START";N
10 D$=CHR$(4) : Q$=CHR$(17):Z$=CHR$(26)
15 FOR I=N TO 9999
20 N$= "0000" + STR$(I):N$= "567" + RIGHT$(N$,4)
25 PRINT D$ "PR#2"
30 PRINT Q$ " " N$
35 IF PEEK(1658) 1/4 128 THEN 1990
40 PRINT D$ " PR#0 "
45 PRINT D$ " APPEND DIALER 567 "
50 PRINT D$ " WRITE DIALER 567 "
55 PRINT N$
60 PRINT D$ " CLOSE DIALER 567 "
65 PRINT Q$ " CHR$(26)
70 REM HANG UP AND BE SURE THAT YOU DID
75 PRINT D$ " PR#0 "
80 PRINT D$ " PR#2 ":PRINT D$:PRINT Z$
85 FOR J=1 TO 600:A= -1:NEXT
90 NEXT
```

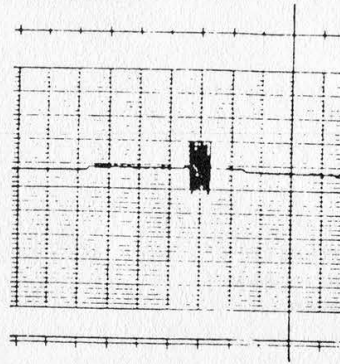


FIGURE 1
Nickel

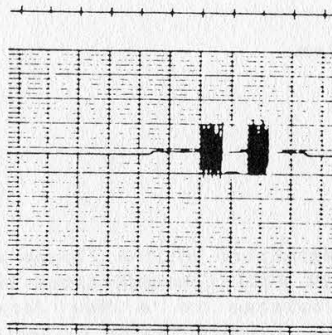


FIGURE 2
Dime

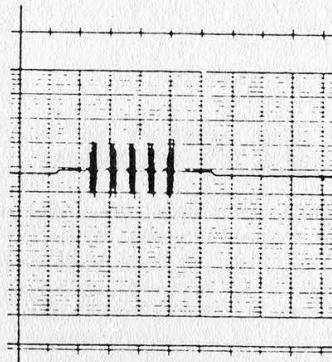


FIGURE 3
Quarter

0 → 1 Second

THESE OSCILLOSCOPE READINGS CAME FROM THE NEW JERSEY BELL INVESTIGATION OF THE PRIVATE SECTOR 2600 BULLETIN BOARD SYSTEM BACK IN 1985. THEY ARE MEANT TO PROVE THAT OUR SYSTEM OPERATOR INTENDED TO DEFRAUD THE PHONE COMPANY BY USING HIS COMPUTER TO IMITATE THE SOUND OF COINS DROPPING INTO A PAYPHONE. THEY DON'T EXPLAIN HOW HE WOULD HAVE DRAGGED HIS NON-PORTABLE COMPUTER OUTSIDE TO A PAYPHONE TO ACCOMPLISH THIS. BUT THEY DO SAY LOTS OF OTHER INTRIGUING THINGS AND WE'VE REPRODUCED ONE OF THE LETTERS FROM THESE TECHNOLOGICAL GENIUSES FOR YOUR ENJOYMENT ON THE FOLLOWING TWO PAGES.

FROM THE 2600 FILES

Bell
Communications
Research

Telephone Network Security
Electronic Toll Fraud - Blue
Examination of Evidence
File-2

August 21, 1985

Mr. R. M. Paprcka
Security Representative
New Jersey Bell
550 Broad Street
5th Floor
Newark, NJ 07101

Dear Mr. Paprcka:

I have completed examination of the floppy disk you brought to the Network Security Laboratory of Bell Communications Research, Red Bank, New Jersey on July 22, 1985. It relates to a New Jersey Bell investigation 2E-0036 involving Thomas Blich, Private Sector bulletin board, Dover, New Jersey.

The 5 1/4 inch flexible disk carries the following notation:

"Disk Number 041
THE CAT'S MEOW
CAT HACKER 3.71
SOUND PROGRAMS
MG31"

The mark "RMP 7/22" also appeared on the label and at the time of my examination I added my mark "BCR-WVH 7/24/85."

The disk was loaded into an Apple II computer and the contents displayed on the screen (Table I.) The program "The Cat's Meow" relates to telephone signals, and its program instructions were listed (Table II.) The purpose of the program is to produce a variety of tones used in the telephone system, including the signals of a Touch-Tone^R dial, the 2600Hz trunk idle signal and the tones of the 2 out-of-6 multifrequency key pulsing (MFKP) code used in the long distance telephone network and the coin deposit signals produced by coin telephone sets when coins are deposited. A tone generator producing 2600Hz and the MFKP signals representing the ten digits and the control signals KP and ST can be used to redirect long distance calls to new destinations while bypassing billing equipment. Such a generator is commonly called a "blue box." A signal generator that simulates coin deposit signals is called a "red box."

On August 13, 1985, Patrolman Michael Grennier, South Plainfield, New Jersey, brought the following equipment to this laboratory:

An Apple IIe personal computer, SN 1303187 equipped with:
Novation Communications Module, 4105J
Hard Disk, XEBEC Mod. 9710F, SN 4-0794
Floppy Disk drives A2M0003, SN 1046016, and 1193212

Patrolman Grennier loaded the program "The Cat's Meow!" from the 5 1/4 inch flexible disk into the computer and pressed the letter D on the keyboard to select the dial feature of the program. Progress of the program was observed on the monitor screen. The audio output was fed to signal analyzing equipment which included a Wilcom Model T180 Tone Signaling FFT Analyzer and a Gould Digital Storage Oscilloscope, Model OS4020 used with a Gould Brush 220 Recorder.

Table III shows the appearance of the screen. Pressing the letter T selects the the Touch-Tone Mode. Patrolman Grennier entered the sequence of number 1 through 0, followed by * and #. The computer produced tones which were analyzed by the Wilcom FFT Analyzer. Its printed output is shown in Table IV. The signals generated are those produced by a telephone set with push-button dial.

Next, Patrolman Grennier pressed the letter M to put the dialer into the multifrequency mode and then entered the sequence 1 through 0, followed by K, S, and \$. Table V shows the analyzer output which identifies the signals as the MFKP trunk signalling code.

Patrolman Grennier then loaded and ran the same program from hard disk, repeating the procedure described above. The results of the measurements are shown in Tables VI and VII. They correspond to the results shown in Tables IV and VI.

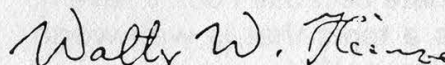
Finally, Patrolman Grennier pressed letters L, M, N in succession. The computer produced one, two, and five tone bursts, respectively. Figures 1 through 3 are representations of these tone bursts captured by the oscilloscope and Brush recorder. Their duration and spacing confirm the intent to imitate coin deposit signals.

Patrolman Grennier remained in control of the Apple computer and associated equipment throughout the test and left with all equipment he had brought after the measurements were completed.

The flexible disk you brought is returned to you herewith.

Approximately 16 man-hours were required to perform this analysis.

Very truly yours,



Walter W. Heinze
Member of Technical Staff
Network Security

NVC-BCR23131-WTH-1j

Atts.
Sworn Statement
Figures 1 through 3
Tables I through VII

SPRINGTIME LETTERS

More Secrets

Dear 2600:

Something that may interest readers and raise a few questions about the US government is the National Coordinating Center located in Arlington, Virginia. This is part of the Defense Communications Agency and is operated by the Pentagon. Its stated purpose is to make available all civilian communication facilities in the time of a national emergency to the Department of Defense. Its staff includes representatives of 12 of the United States' largest communications companies, including MCI, Comsat, ITT, GTE, and of course, AT&T, as well as members of various federal agencies.

The President can, in times of what's termed a "606 Emergency", take control of any communications facilities if he thinks it is necessary to the "national defense". This power was given by the Communications Act of 1934, and the NCC, which was created in 1984, is the place that would allow this to happen.

If readers want more information on the NCC and some of the actions that make it more threatening than its intended purpose, there was an article written in a mid-1987 issue of *Omni* entitled "National Guard". I can't leave the exact date because I don't have it. But this is a topic that is well worth informing yourself of.

Hopefully, awareness will grow about the potential for abuse that comes from the capability of controlling much of the public's sources of information, as our political system becomes increasingly intertwined with new technologies and their applications. 2600 should be praised for its efforts in educating people in this field of thought.

Doom

Encouraging Words

Dear 2600:

I figured you might get some cynics writing in saying they don't like the new quarterly format. So I thought I'd write and say that this new format looks just great to me. Keep up the good work!

A Friend in Texas

Obviously you had to have written this letter before this issue was ever published. So how you were able to tell it would look so nice is beyond us. We have to say, however, that we're pretty pleased with the way it came out too.

Still More Secrets

Dear 2600:

I am not a subscriber, but I was wondering if you could give me some info on the following things:

First, have you heard of a system called "Terac"? It's based in Sacramento, California and is massive! The memory as calculated in megabytes is as follows: $10E+100+10E+100+10E+50$. As far as I know it is used by military for a temporary storage. An example of a logon would be: Password: madness, ID: 25813, security level code: mad 532, security level code 2: ness 532. (Note: these numbers change after each login randomly.) Security level codes are three alpha and three numbers or three alpha, two number, and one more alpha.

The second system logs on saying it is "Marbles BBS" and operates like a regular (but weird) BBS. The following commands are available: A=answer call, B=??, C=??, D=??, E=e-mail, S=send letter, R=receive letter, M=make call, Q=quit. However, if you mess around with it enough, you'll get asked for a password. After getting through 15 passwords, 20 identification numbers, and 62 levels of access, the system

tells you it is the "Military Operations Unit System" and then the Artificial Intelligence kicks in. Then from there if you were to tell it to "launch missile", it will ask you what type of missile, target, from where, etc. Then it will start a countdown. I stopped it before zero but I was wondering, could someone really launch the missiles? Isn't there a human factor involved?

If you know about these systems, or know anyone who does, please write me some notes on them. Terac traces all calls coming in, and both systems have artificial intelligence to some extent. Terac accepts ROM dumps but MOUS doesn't. MOUS doesn't trace or anything and the two systems are linked. (You will not find out by using them—I didn't.) But if you get busted (I did), they will usually just tell you to stop calling.

Also, have you guys figured out how NASA ciphers all their shit? I can get in but I can't read anything.

First of all, we appreciate your stopping the countdown. Second, since your letter didn't bear a Yale postmark, we assume it's serious. Somehow you managed to get through 62 levels of access to the missile launching program and you're asking us if WE know anything about these systems? Either this is an incredible case of exaggeration or it's another test of our patriotism (will 2600 help overthrow the government or will we run and tell the good guys about the bad guys without ever suspecting that they're really one and the same, etc.). On the off chance that what you're saying is true, you're better off showing us what these systems can do rather than waiting until it's too late or telling the wrong person. Anonymity guaranteed.

A Very Special Number

Dear 2600:

Now that Jerry Falwell has disconnected his 800 number, callers may wish to dial the National Rifle Association at 800-368-5714. They only answer between 8:30 and 5 Eastern Time, Monday through Friday. But the firm that does their telemarketing can be reached 24 hours a day at 800-535-3200.

What a wonderful public service....

Tales of Hackers

Dear 2600:

Enclosed is another newspaper article about someone hacking MCI codes and getting caught after the calls were traced back to his apartment. To top it off, he also got busted for the pot plants on his balcony. Some people never learn from other people's mistakes and seem to have to find out first-hand.

I found a goody in An Introduction to

Police suspect UT hacker stole long-distance codes

By John Harris
Associated Press Staff

Police suspect a University of Texas student who was arrested for stealing a home computer to call a long distance telephone company 14 to times in the past few days and illegally obtain 16 codes for long distance calls.

Charges had been filed Tuesday against the 21-year-old UT Austin man, who police believe ran a computer hacking system from his Austin, Texas apartment for about two months.

Police believe his home computer may have called an MCI computer in Austin as many as 14 times in the past few days, said police Sgt. Robert Ansley. A list of calls was made to trace 14 of the calls. He said police found a small, older model home computer in the man's apartment.

That was the thing about it. It was just a cheap old computer system, Ansley said.

The man, a student from El Paso in the college of natural sciences at UT, had a list of two pages of access codes from MCI, Ansley said.

Police suspect the calls from his home were made to MCI to get access codes. The computer would dial MCI every 30 seconds, try a long distance number to see if the code would work, and record the code if it was valid, Ansley said.

The codes could be sold to other people who could use them to make free long distance calls or to others with similar computer operations in different parts of the country, he said.

Ansley said police would have to research each code to see if it was valid, Ansley said. He said 16 valid MCI codes were taken from the Austin area were found, along with at least 100 codes from other long distance carriers.

Ansley said he was aware of what was happening through MCI computers, which are designed to detect fraud. MCI said the telephone officials, who contacted police, Ansley said.

The man also faces misdemeanor charges after police found marijuana plants about 1 1/2 feet tall on his apartment balcony, Ansley said.

The man remained in City Jail late Tuesday.

Cedar Park treasurer for Fire Department charged in fraud, theft

By Scot Meyer
Associated Press Staff

CEJAR PARK — The assistant treasurer of the Cedar Park Volunteer Fire Department is being held in the Williamson County Jail on charges of burglary and theft, officials said Tuesday.

Ronald Keith Harp, 22, of 8011 A Lane, Sharp Drive in Cedar Park, was charged with two counts of burglary by passing and two counts of theft, according to the jail, officials said.

According to Williamson County Sheriff Deputy David Moore, Fire Department officials reported that between Aug. 27 and Oct. 4 several department checks were altered or forged. Department funds were diverted to other accounts and by the time the alterations were caught, about \$2,000 was made payable to the Cedar Park Volunteer Fire Department and a check issued to the Cedar Park Volunteer Fire Department was missing.

Walter Davis, president of the Cedar Park Volunteer Fire Department, declined to give details on the charges or say how much money was believed to be missing.

He would comment on the situation at a later time, he said.

(continued on next page)

LETTERS OF THE SPRING

(continued from previous page)

Operating Systems published by Addison-Wesley, a short PL/I program to lock up a computer running under OS/360.

REVENGE: PROCEDURE OPTIONS (MAIN, TASK);

WAIT(EVENT);

END REVENGE;

Supposedly this makes the computer wait for something that won't happen and tie up the system. I have not had an opportunity to test it myself.

The Hooded Claw

Advice Wanted

Dear 2600:

I have recently subscribed to your magazine because I am starting an "on call" personnel business, screening potential employees.

Frankly, I am quite new to computers, but am determined to get a set-up which will enable me to conduct business from my home.

I am wondering if there are any people around who could help me in this regard by telling me what software to purchase and how to gain access to public records in all states, for background check purposes.

Some of the types of things I want to access are county records, federal court records, worker's comp records, and driver records.

The process through the mail (which most governmental agencies make available) is very slow.

I am also interested in obtaining any other personal background information (credit history, military records, assets).

If there is a publication with access codes, etc., please let me know about it, because I really want to get this business going.

It sounds as if you want to bypass the system and do things efficiently. Often, this means bending or even breaking the laws. You won't get anywhere if

you depend on publications that print access codes. You want exclusive access to your sources. If you have to share this access with anyone who can get their hands on a publication, it just won't be effective. We distribute information but there is a limit to how far we can go. If we were to print passwords or codes (despite the fact that it's illegal), so many people would use them that they would soon get shut off or monitored very closely. For that kind of information and the kind we suspect you're after, you need to make personal contacts—through the mail, on the phone, on bulletin boards, or on the street. You'll have to use your instincts insofar as who you trust and what information appears valid. If we've misread your question and you actually want to do this by the book, we're sure it's possible. Simply go through the agencies involved. But, as you've already noted, that tends to be slow, and quite often expensive.

Of Phones and Politics

Dear 2600:

The importance of the telephone in modern life became apparent in the recent New Hampshire Primary Debate of the Democratic party. The first question asked by the moderator was directed at Senator Paul Simon in reference to the Senator's proposal to put free telephones in the homes of those who could not afford them. He would place a two percent tax on long distance charges to pay for this program. Bruce Babbitt attempted to discredit the proposal by challenging Simon to address the broader issue of the deficit. Gary Hart tried to ignore the subject altogether but Representative Albert Gore showed himself to be the most knowledgeable "telecom enthusiast" seeking the nomination by attacking the Reagan administration's policy of local "access fees" to

subsidize long distance service for big businesses. Gore also stressed the need of making telephones affordable to the widest base of people possible. Telecom may be on the agenda, but we're waiting for a candidate who will support 2600's campaign against touch tone fees!

Skinhead Steve and The Boy

You'll be waiting a long time unless you start telling them about it. Politicians know frightfully little about high tech; they need people like us to explain it to them. A well worded letter to your elected official explaining why the touch tone fee is a ripoff may yield surprising results. What have you got to lose? By the way, if any readers need the facts on the touch tone fee, we suggest thumbing through our 1987 issues.

More on the 8038

Dear 2600:

Not to drag the 8038 issue into the ground or anything, but....

The ICL8038 is still in production and fairly easy to get if you just look around a bit.

For complete data, call (408) 996-5000 and ask to be sent the 1987 Component Data Catalog.

Although you-all have no control over what people advertise in your *2600 Marketplace*, \$7.50 for one 8038 is ridiculous!

REMOB Hunting

Dear 2600:

The attached is from William Poundstone's *Bigger Secrets*. I'm interested in the reference to "REMOB" on page 84 and on other surveillance techniques.

The ultimate in phone spying is REMOB, remote observation. The phone company is said to have certain secret numbers—one is in Iowa—that can be used for listening in on other

numbers. You call the REMOB number with a touch tone phone, then punch in two access codes and the phone number you want to tap—which can be anywhere in the country. The tapping is done by a sophisticated technique that does not create a telltale click, hum, or beep. It's all done automatically, without an operator, and anyone knowing the number and access codes can spy on anyone anywhere."

I don't recall ever seeing "REMOB" addressed in the newsletter. Can anyone add to it?

MH

Uniondale, NY

We have yet to see specific evidence of a working REMOB. But we do believe their existence is possible, certainly from a technical view. It's doubtful that one system could spy on numbers across the country because of the many different systems still in use. If and when all of the phone networks become integrated, such a concept will be very possible. For now, we will offer a reward of \$100 for the first person who comes forward with a working residential REMOB. That ought to settle matters, one way or the other.

The Global Village

Dear 2600:

In the October 1987 issue of *2600*, you wrote about how people from all over the world wish to run electronic bulletin board systems under the name of *2600 Magazine*.

Here are my ideas: enlist the aid of hackers and phreaks from *all over* the world to write a combined version of Diversi-DIAL and Fido for all major brands of personal computers. Second, since this is supposed to be like a global village setting of telecommunications hobbyists for the Communications Revolution, why not subtitle it Foundation after Dr. Isaac Asimov's

(continued on next page)

LETTERS

(continued from previous page)

Foundation novel?

Because what you are trying to do is gather people and data together to create a digital sanctuary for ensuring freedom of speech, especially now since advancing technology allows us to use that basic freedom to reach more people than ever before. That is sort of what the *Foundation* novel was about.

I hope the hackers and phreaks of the world are willing to write this much needed BBS software, because too many of us are kept apart by the telephone systems of our countries. For if we *really* wish to learn and finally *control*, we need common places where we can go to draw on and then expand our knowledge.

The NATO Association

We need as many methods and channels of reaching people around the globe as our imaginations permit. The computer/telecommunications revolution can be mankind's salvation or doom. We're helping to make that decision.

Got a letter for us? Send it to: 2600 Letters, PO Box 99, Middle Island, NY 11953.

AT&T ALLIANCE[®] Teleconferencing Services

TO SET UP CALL YOURSELF

Dial 0 + 700 + 456-1000* on any touch-tone phone. A recording will tell you when to:

1. Enter the total number of locations, including yours.
2. Dial the first number. United States: + area code + local number. International: + country code + city code + local number.
3. Repeat step 2 for remaining numbers. Then **firmly press** to add yourself.

*Available in most U.S. locations. For operator set-up or if you have difficulty accessing ALLIANCE Service, call 1 800 544-6363.

GENERAL TIPS

During set-up Dial <input type="checkbox"/> to continue Dial <input type="checkbox"/> if: • Busy, no answer • Make a mistake • Poor connection Dial <input type="checkbox"/> for assistance	During the call Dial <input type="checkbox"/> to: • Add locations • Reconnect locations • Leave/rejoin call Dial <input type="checkbox"/> <input type="checkbox"/> for assistance
---	--

TO SET UP CALL WITH MEET-ME

1. Dial 1 800 544-6363. An operator will ask the date, time, call duration, number of locations and method of billing.*
2. You will be given two special access numbers. One you will keep, the other you will give to your fellow conferees.
3. At the meeting time, everyone calls their special access number and is automatically connected together. Only you are required to use a touch-tone phone.

*You may want to accommodate those who call in early by reserving a start time five minutes prior to the time you've scheduled the meeting to begin.

FEATURES

To add locations (domestic or int'l.) Dial <input type="checkbox"/> if you have already reserved space Dial <input type="checkbox"/> <input type="checkbox"/> if you have not reserved space Dial <input type="checkbox"/> if: • Busy, no answer • Make a mistake • Poor connection	To screen callers Dial <input type="checkbox"/> to speak with caller Dial <input type="checkbox"/> to add caller Dial <input type="checkbox"/> to disconnect caller Dial <input type="checkbox"/> to reconnect yourself
---	---

GENERAL TIPS

Dial <input type="checkbox"/> <input type="checkbox"/> to: • Extend call time • Request assistance	Dial <input type="checkbox"/> to: • Leave call • Rejoin call
--	--

Attention Readers!

2600 is always looking for information that we can pass on to you. Whether it is an article, data, or an interesting news item—if you have something to offer, send it to us!

Remember, much of 2600

is written by YOU, our readers.

NOTE: WE WILL ONLY PRINT A BY-LINE IF SPECIFICALLY REQUESTED.

Call our office or BBS's to arrange an upload. Send US mail to

2600 Editorial Dept.

Box 99

Middle Island, NY 11953-0099

(516) 751-2600



RCI CORPORATION • 533 METRO PARK • ROCHESTER, NEW YORK 14623 • CUSTOMER SERVICE 1-800-825-2733

ACCOUNT NO.

BILL DATE

02/26/88

PAYMENT DUE BY

03/25/88

002944

H

MAKE CHECK PAYABLE TO:

RCI CORPORATION
P.O. BOX 20401
ROCHESTER, NEW YORK 14602

AMOUNT ENCLOSED

0.06

PAY THIS AMOUNT

PLEASE RETURN THIS FORM WITH PAYMENT TO ENSURE PROPER CREDIT

EVERY MONTH WE GET A FOUR-PAGE BILL FROM RCI FOR SIX CENTS. IT'S BEEN GOING ON FOR WELL OVER A YEAR NOW. FORTUNATELY, THEY DON'T SEEM TO MIND THE FACT THAT WE'RE DELINQUENT IN OUR PAYMENTS. NOT TO MENTION THE FACT THAT WE CAN'T EVEN REMEMBER EVER USING RCI IN THE FIRST PLACE.

ROLM Phone System

The next time you find yourself cursing and swearing at the telephone because it's gotten too complicated and bureaucratic lately, keep in mind that it could be worse. You could be at the State University of New York at Stony Brook.

Being relatively close to our offices, we've been able to follow this story rather closely. We don't doubt that similar escapades are occurring all over the country and will continue to do so in the future. We'd certainly love to hear about them.

In The Beginning

Up until 1987, using the telephones was very simple. The phone system at Stony Brook was a Centrex operated by New York Telephone. Everyone on the campus used the 246 exchange. To reach the main switchboard, you would dial (516) 246-5000 from the outside world. To reach the old, antiquated UNIVAC computer system, you'd dial (516) 246-9000 from off campus or 6-9000 from on campus.

Most of the phones were rotary dial. Callers simply dialed 9 to get outside access unless their lines were restricted to on-campus only.

It wasn't the best of systems by far. It was slow and old fashioned. But it did work. And most people had little trouble understanding it. Eventually though, everyone knew that there would have to be a change.

In 1986, the university began installing a brand new phone sys-

tem: the ROLM CBX II 9000. This would be the system to bring the campus into the information age, with useful features and high speed data capabilities.

There would be a transitional period. The 246 exchange would be phased out over a period of two years and the 632 exchange would be created. The neighboring University Hospital (using the 444 exchange) would switch from its Northern Telecom SL-1 switch to the ROLM system in 1987. The entire campus, student dormitories the last to go, would be cut over to the ROLM system by Fall 1988.

But it didn't work out in quite that way.

Of course, no one in their right mind would expect such a project to be 100 percent on schedule. But not even the pessimistic were able to predict the incredible range of problems and foul-ups that the ROLM telephone system would bring to Stony Brook.

To start with, a certain amount of "culture shock" has to be expected whenever something new is introduced. This is why it is essential for something like a phone system to be easy to grasp as well as logical. Unfortunately, the ROLM system has been neither, at least not for most average people.

The first sign of trouble came in the form of a memo from the Communications Department at the university. All answering machines, modems, speaker-phones, and anything else that

Creates a Nightmare

hooked into a telephone would not work on the new system--at least not without an expensive digital-to-analog conversion device. So everybody had to conform to the same system.

Modem users had to obtain a special device that hooked their computer into the "modem pool". All data calls had to be placed through the modem pool and no longer from individual lines. Incoming calls were more complicated. Callers could no longer just dial the phone number of the computer they wanted. They would have to dial 632-8000 to connect to the modem pool and then enter another five-digit number before being connected.

Instead of using answering machines, everyone was forced to use the ROLM Phonemail System,

"It's reached the point where I dread hearing the phone ring. I'd say at least a third of the time something goes wrong somewhere along the line."

a voice message system that is fairly flexible, but not a true replacement for one's own answering machine. Messages do get lost, mailboxes get full much faster than answering machine tapes, the system is easy to break into mainly due to three-digit default passwords and the fact

that Phonemail provides a fairly complete listing of mailbox extensions after hearing a few stars from a touch tone phone. Plus the very simple fact that it just isn't tangible.

To leave a message for someone, the caller had to either dial the number that was hooked into Phonemail or a number that forwarded to Phonemail. Or they could dial 632-6601 and choose the five-digit extension they wanted to leave a message for. To retrieve messages, the Phonemail subscriber would dial 632-6600, enter his extension (or name), and password. Not quite the same as pushing a button on an answering machine. The advantage of course is that messages could be heard from any location. The disadvantage is that they could be heard by any person.

More Problems

On most key phones (office phones with several line buttons), you would answer the phone by picking up the receiver and punching in the ringing line button. That is known as a logical, not to mention traditional, way of doing things. Why the ROLM people chose to abandon this simple way of answering the phone is completely beyond us. As office workers and professors throughout the campus have found out, picking up the phone the "old" way will immediately disconnect the caller.

It is true that the university

(continued on next page)

ROLM System Horrors

(continued from previous page)

offered training classes on how to use the new phones where this change in phone logic was emphatically pointed out. And it is true that the 88-page phone manual made note of the fact on page 4. But a great deal of people still thought they could answer phones without reading manuals or going to classes. The reality of the matter was that thousands of potential phone-answerers would have to be trained and retrained. And even then, mistakes would be common.

"It's reached the point where I dread hearing the phone ring," an administrative office worker says. "I'd say at least a third of the time something goes wrong somewhere along the line. And a lot of the callers get angry. Who can blame them?"

New telephone numbers were assigned on the ROLM system with little or no input from the phone users. Instead of assigning easy-to-remember numbers for commonly dialed offices and services, it was, with few exceptions, done sequentially--either alphabetically or by location. For instance, campus information used to be reachable at 246-3636. Now, everyone must remember 632-6830.

Under the old system, the campus radio station was able to provide a school closing hotline. Callers would dial a number and hear a listing of schools that were closed because of adverse weather. Only one caller at a time could access this information.

Under the new system, this service had to be switched to the Phonemail system. But because ROLM had never installed any kind of a limiter on Phonemail, the entire system would get tied up whenever more than ten callers dialed in. No one could get into their voice mailboxes or leave messages. So the school closing hotline, an undeniably valuable service, was shut down by the university.

Even the university's main switchboard was affected by this. They could no longer put a recording on when the switchboard was closed because the same problem of overcrowding would occur. At presstime, after-hours callers to either the old 246-5000 main switchboard number or the new 689-6000 main switchboard number get a nonsensical Phonemail recording that even gives away a "secret" internal extension number of the main switchboard, as well as the hidden ID of their Phonemail account! Technology marches on.

Another change everyone was forced to live with was the denial of access to outside operators. Because the new system uses tie-lines to make outside calls, operators have no way of verifying the actual telephone number the caller is dialing from. Access to New York Telephone and AT&T operators was therefore cut off.

This meant no third party, collect, or otherwise operator-assisted calls were possible. It also

(continued on page 34)

NEW DIALING INSTRUCTIONS

On August 15th the first phase of the ROLM Telephone System Installation will cut over. This will include the replacement of all Centrex ("246" exchange) telephones on Main Campus, excluding student dormitory telephones. This first cutover will also include replacing approximately 50 Centrex lines existing in the Health Sciences Center. As a result of this initial installation, the University will be served by three separate telephone systems.

The new exchange for Main Campus will be "632". The exchange for the Health Sciences Center and University Hospital will remain "444". The Residence Halls will remain on the "246" (Centrex) exchange until August, 1988.

Please read the dialing instructions outlined below which pertain to your telephone system.

The Main Campus Switchboard Number will be 689-6000. To call individual extensions (Direct Inward Dial, or "DID" Extensions) from off campus, dial "632-XXXX" (X = the appropriate extension number).

The University Hospital Main Switchboard Number will remain 689-8333. To call individual extensions (Direct Inward Dial Extensions) in the Health Sciences Center and University Hospital from off campus, dial "444-XXXX".

ROLM TELEPHONE SYSTEM USERS

On Campus Dialing—The "246" exchange has been changed to "632"

To call any "632" exchange on Main Campus
Dial "2 + XXXX"

To call any "444" exchange (HSC or Hospital)
Dial "4 + XXXX"

To call remaining "246" exchange (Student Residence Halls)
Dial "9-246 + XXXX" (These calls will be routed over tielines)

Some ROLM telephones have five-digit "Non-DID" extensions, such as "5-XXXX" or "2-0XXX". These extensions can be dialed directly from on-campus locations only.

Off Campus Dialing

Dial "9" + listed telephone number (including area code if required)

International Calls—International calls can be placed without the assistance of the International Operator by dialing the call directly from a ROLM telephone:

Dial "9 + 011" + Country Code + City Code
(See International Code listings at end of directory)

Emergencies— Public Safety—Dial "333"
Fire Safety—Dial "333"
Ambulance—Dial "2 + 8888"

Campus Operators

Main Campus—Dial "0"
Hospital—Dial "4-0"

HEALTH SCIENCES CENTER AND UNIVERSITY HOSPITAL

The few remaining Centrex phones on the "246" exchange in the HSC will be replaced with ROLM telephones and the exchange will be changed to "444" (All exchanges in the HSC and Hospital will be "444"). ROLM system users should follow the dialing instructions above.

SL-1 SYSTEM USERS

On Campus Dialing

To call a "632" exchange on Main Campus:

Dial "9-632 + XXXX"

(These calls will be routed over tielines)

To call a ROLM telephone in the HSC Dial "4 + XXXX"

To call an SL-1 system extension (444-XXXX):

Dial "XXXX"

To call a "246" exchange: Dial "9-246 + XXXX"

Emergencies — Public Safety (HSC)—Dial "2502"
Public Safety (Main Campus)
Dial "9-632-3333"

Campus Operators Hospital— Dial "0"
Main Campus—Dial "9-632-0"

STUDENT DORMITORY CENTREX USERS

The Centrex "246" exchange will remain intact until August 1988. There will be tielines available for those users without Unlimited Local Service. The access code for these tielines will be "122".

On Campus Dialing—

To call another "246" exchange (Student Dormitories)
Dial "6 + XXXX"

To call a "632" exchange on Main Campus:

Dial "122-2 + XXXX"

(If you have Unlimited Local Service:

Dial "9-632 + XXXX")

To call a "444" exchange in the HSC or Hospital:

Dial "122-4 + XXXX"

(If you have Unlimited Local Service:

Dial "9-444 + XXXX")

Emergencies— Public Safety—Dial "6-3333"
Fire Safety— Dial "6-3333"
Ambulance— Dial "122-2-8888"

TELEPHONE REPAIRS FOR ROLM SYSTEM USERS

Between the hours of 8:00 a.m. and 5:00 p.m., all mechanical difficulties with your telephone should be reported to the Campus Repair Operator by dialing "5-0503" (cannot be dialed directly from off-campus). Please do not call telephone repair for installation, changes, or relocation of your telephone. Service of this kind must be ordered in writing through the Office of Communications Management Engineering, Suffolk Hall, Room 146, (2-6130). New Telephone Work Request Forms will be distributed in the near future.

TELEPHONE REPAIR FOR STUDENTS

The procedure for reporting telephone repairs for Residence Halls (Centrex) telephones will remain the same. To report trouble on the telephone line, contact the New York Telephone Repair Bureau by dialing 9-611. Students who purchase their own telephone are responsible for its repair or replacement. If the telephone is leased from ATTIS, it may be dropped off at the nearest AT&T Phone Center for repair.

DIALING INSTRUCTIONS ■ iii

THESE INCREDIBLE INSTRUCTIONS APPEARED IN THE STATE UNIVERSITY OF NEW YORK AT STONY BROOK'S TELEPHONE DIRECTORY AS THE NEW ROLM PHONE SYSTEM WAS BEING INSTALLED. WE CHALLENGE ANY OF OUR READERS TO SHOW US AN EASIER WAY TO SUMMON AN AMBULANCE THAN DIALING 122-2-8888.

The ROLM College Campus

(continued from page 32)

meant that non-direct-dialable overseas calls were impossible. Technically, the campus operator can hook callers up to a real operator, but is reluctant to do this most of the time. Besides, campus operators are gone at 4:30 pm and all of the weekend. Since Stony Brook consists of a very large number of foreign students who need to call strange countries at weird hours, we can only hope that when the dormitories are hooked in later this year, operators will be accessible. If something isn't changed by then, an incredible hardship will face such students. The only possible way to make such calls will be by dropping money in a payphone (calls cannot be charged to the 632 exchange) or by finding another number to charge the call to from a payphone.

But operators are only one of the basic services that have been denied to users of Stony Brook's ROLM system. The 976 dial-it exchange is unreachable from any phone. This is becoming common in institutions, but the fact remains that there are many legitimate uses for dial-it services. A simple task like setting a clock is now very time consuming and frustrating. And when the dormitories are cut over, will all students be prohibited from dialing Sportsphone or their horoscopes from their own phones?

Equal access rights have been all but denied to the phone users. The system will not allow you to

place a call through a carrier of choice unless the 950 exchange is used, in which case the call can't be billed to the originating number. And the 950 exchange is unreachable except on lines with long distance access. This is stupid, since 950 is toll-free and allows callers to charge calls to their own accounts. Toll-free 800 numbers, on the other hand, are accessible on all outside lines. It seems obvious that the programmers don't understand the concept of 950 numbers. As a result, the end users are inconvenienced.

Some local exchanges are also unreachable because the people who program the switch haven't gotten around to entering them, despite numerous reminders and requests from users. The 474, 476, and 696 exchanges have all been around for many months now. Without a long distance line, you cannot access these local exchanges.

Nightmares

But far and away the worst aspect of the ROLM CBX at Stony Brook is the outages. Despite the fact that they're not supposed to happen, they do. Quite frequently. Sometimes only for a couple of seconds, sometimes for a couple of hours.

Under the old Centrex, you could always get a dial tone. Even if the power went out, the phone lines were there. Now, whenever something goes wrong, everything is frozen. No incoming calls. No outgoing calls. No on-campus

Incomprehensible Bureaucratic Mess

calls. No data communications (remember, everything has to go through the modem pool). No intercoms (the phone system now incorporates these, too). No answering machines (thanks to Phonemail). Complete and total integration. Complete and total paralysis.

Recently, University Hospital had a serious outage. Nobody was able to dial anything. Eventually, if not already, this system will claim some lives.

Occasionally, in the words of a ROLM switchroom employee, preventative maintenance requires the phone system to come down. And that is where the engineering and human perspectives of telephones come into conflict. Phone systems cannot be treated as if they were large, multi-user computer systems that occasionally crash. Phones are different--they are vital and personal.

Uselessness

To this day, the vast majority of phone users do not use most of the features of the phone system, either because they have no idea of how to use them or because they have no desire to. As a result, most of the phones have at least four completely useless buttons on them. If the user wants a different configuration of buttons incorporating those features, that they *can* use, they're told that it's "not possible". That's not what ROLM or the university said before the system was installed. ROLM itself has inhibited the potential of its own

system by discouraging user programming.

The most useful feature on the system is the Repertory Dialing button. It's like a speed dial button except it can be programmed to incorporate all kinds of other features. In other words, one "repdial" button can duplicate any other feature button or combine several features, or do something entirely different. A few of these buttons would allow for great flexibility for users. But getting more than one of them is completely impossible. A potentially positive application is therefore turned into yet more frustration.

Call picking is another feature that could be useful for some. If a phone is ringing and you can't get to it, you simply hit the "pick" button and enter the extension that's ringing. It will then magically appear on your line. The only problem with this is that there's no stopping it! As long as someone knows the number of a ringing extension, they can divert it to their line. Call picking can also be used to snatch calls that are on hold, although that "feature" isn't documented. This kind of a feature works fine in offices where everyone is presumably working towards the same goal. But on a college campus of more than 20,000 people, this "kidnap" ability is ill-considered and dangerous.

Although it has lots of unused potential, the ROLM CBX II 9000 is, by and large, poorly designed for offices. A simple feature like

(continued on next page)

ROLM System Horrors

(continued from previous page)

distinctive ringing is common in today's phone systems; you'll even find it in cheap two-line phones at Radio Shack. But not here. You can change the way the ring sounds, but all lines will sound exactly the same on the same multi-line phone. You can't even turn one line off and leave another on! The only way to have access

narios. It is vital not to be dependent on any form of technology because when it fails, you will be crippled. This is a very basic rule that is being followed less and less. How many of us have lost hours of work into thin air because of a computer glitch? Something as crude as a printed copy of our work could have saved us so much trouble. Crude backups must also exist on our new phone systems so that when they do unpredictable things, we'll be able to get access to the basics, like an outside dialtone.

NOTE

Once you have lifted the receiver to answer a call, do not press the line button. Doing so will disconnect the call.

What's particularly unfortunate in the Stony Brook/ROLM scenario is the pairing of a huge corporation with a huge bureaucracy. A simple human being is no match for this ugly combination. He is thus pushed around and forced to alter his way of doing things because that is the way it has been decreed. In reality, he should be the one running the show.

to all of the lines in your office and have distinctive ringing for each is to have a different instrument for each line. Truly brilliant.

For those that have realized that ROLM doesn't provide all the answers and causes a good deal of the problems, the university administration bureaucratically forbids users from installing their own systems or even individual phone lines. This creates an inconvenience--and a danger.

As we said earlier, what's happened at Stony Brook is happening in other places. It represents something scary about our emerging technology. While great things are possible, so are big problems. And nothing will lead to disaster quicker than an unwillingness to prepare for those worst-case sce-

Clearly, more user participation is essential, both in the choosing of an institutional phone system and in its operations. These systems must be designed based on comments and suggestions from the ordinary users, not just those who understand all the computer/phone jargon. The corporations and the institutions have got to start listening and acting swiftly to correct mistakes and inadequate facilities.

Otherwise, an increasing number of us will become disconnected altogether.

HAPPENINGS

The big story in the phone industry lately seems to be the most recent consumer craze: call blocking. This is basically a service that shuts off access to certain dial-it numbers, largely a response to the pornographic services being offered on many of those numbers.

In Idaho, the plan has been approved for customers connected to exchanges equipped with digital switches. They will be able to block calls to the 976, 430, and 499 exchanges, as well as calls to the 900 nationwide numbers. For the first 90 days, there won't be a charge.

In New York, the plan is to take effect in April. Customers will be able to block access to the 550 and or 970 exchanges without paying a fee for the first 90 days. After that, they'll have to pay between \$5 and \$10. The 550 exchange currently handles group-calling services, also known as anonymous conference lines. The 970 exchange will be altered to house primarily adult-oriented messages. The 976 exchange would not be blocked but would not contain pornographic material, as it does now.

New York Telephone is also planning to expand its dial-it network tremendously. Last year, they operated 59 message lines. They're now planning on expanding that to over 300.

Meanwhile, the House of Representatives has voted against an outright ban on so-called "dial-a-porn" telephone messages. By a vote of 200 to 179, the House decided it would be better for such calls to be blocked technically rather than banned altogether. Such a banning could be interpreted as a violation of freedom of speech.

U.S. West has established a separate 960 exchange for adult messages rather than have them on the 976 exchange. They also won't provide billing and collection for the 960 service, although they'll supply vendors with the information necessary to do their own

billing.

Customers in that region will also be able to block either exchange.

Bell Atlantic is creating a separate exchange for conference services and adult messages. But they've decided to block all calls to that exchange unless the customer requests otherwise. This "unblocking" service will be free. It will be interesting to see how many people will "register" their pornographic calls with the phone company.

AT&T is eliminating financial incentives to vendors who lease its dial-it service lines in the 900 area code. This is seen as an attempt to eliminate the pornographic services that are found there.

Throughout all of this, everyone seems agreed upon one point. Phone companies cannot refuse to transmit messages regardless of their content. The constitutional guarantee of free speech does not allow for this. When will we start to apply this to computers, specifically computer bulletin boards?

Recently, the Supreme Court ruled that student newspapers could be censored by school administrators without interfering with anyone's freedom of speech. We're damned if we can figure out how this is possible. We also think computer hackers and technically literate people can lend a valuable hand in challenging this dangerous precedent.

How many of us have access to computers and printers these days? Not enough, but undoubtedly a growing number. Every kid going to school today that has a computer and a printer in his home or even in his school is a potential newspaper editor. Even something as crude as a one page dot matrix printout can be considered a newsletter. Because of this, it's suddenly incredibly easy to put out a newsletter and distribute it in school. And what can be done about it? Very little, short of martial law.

(continued on next page)

HAPPENINGS

In this way, we can use technology to express ourselves openly and keep from being manipulated and silenced. If you think you're capable of publishing such a newsletter, do it. Encourage others to join you or compete with you. Offer to use your computer to help give a voice to others that may not have computer access. You don't need school money anymore. You don't need school permission. All you need is imagination and a willingness to grab your rights. There are plenty of other people who want them.

Drug dealers that use beepers have been having some embarrassing moments. A New Jersey dealer had been arrested on cocaine charges when his beeper went off, displaying the number of the person calling. Police called the number and talked to a gentleman who wished to purchase drugs. And guess what those clever cops did?

The beeper is currently sitting on the Camden County Prosecutor's desk. It's still getting calls and the police are still returning them. "We live in a high-tech society," a police officer mused. "Criminals are just as aware of that as we are. These guys are sophisticated. They work very hard at their trade, illegal as it may be."

We've all heard something about computer viruses by now, most of it undoubtedly inaccurate. Israel, Pakistan, the United States—they're in existence in all kinds of places. And they can screw things up pretty good. We're working on getting an in-depth article on viruses, complete with examples, together for a future issue. In the meantime, there is no reason to panic. The only people who will have their lives ruined by computer viruses are those that don't take basic safeguards such as backing up and printing out. Once you become completely dependent on a computer, any computer, it's only a

(continued from previous page)

matter of time before a valuable lesson comes your way.

6,900 AT&T customers in New Jersey are being sent 10 extra copies of the AT&T credit cards they ordered. Last month, a runaway computer at AT&T's credit card center in Piscataway sent out, in separate envelopes, the extra cards.

This is apparently what happened: Some customers complained that they had ordered cards and not received them. To find out if there were more such people, AT&T technicians searched the card division's computer files and came up with a list of about 7,000 names and addresses. The list was "run" on an AT&T computer one day in late December to produce electronic orders for the cards. The list should then have been taken out of the computer. Instead, it was left in and continued to run for 10 more days, generating orders for about 10,000 unneeded cards a day.

People who ordered cards got their order, times 11. So people who asked for one got eleven, those who asked for two got 22, etc. Altogether, nearly 100,000 unwanted cards are crawling through the postal service, each in their own envelope.

Our heartiest congratulations to *The Wall Street Journal*, for adopting the 2600 approach to telephones. A recent article about hotel phones noted that most hotels use timers to charge for calls. The timers, according to the paper, don't click on until about 45 seconds after the caller picks up the phone. "If you call home and say 'I'm here,' and hang up immediately, you probably won't be charged," the *Journal* quotes a major hotel senior vice president. "I wouldn't want that to get much publicity, but it's true." The article also notes that hotels remove telephone

(continued on page 40)

State of Florida

Commissioners
KATIE NICHOLS, CHAIRMAN
THOMAS M. BEARD
GERALD L. (JERRY) GUNTER
JOHN T. HERNDON
MICHAEL MCK. WILSON



DIVISION OF CONSUMER AFFAIRS
GEORGE B. HANNA, DIRECTOR
TOLL FREE 1-800-342-3552
(904) 488-7238

Public Service Commission

**THIS IS A SPECIAL ADVISORY
FROM THE FLORIDA PUBLIC SERVICE COMMISSION
PLEASE READ CAREFULLY!**

Florida has recently experienced the creation of "Pyramid Scheme" and/or "Flat Rate" long distance telephone companies. These companies advertise that through their company you can make unlimited calls from anywhere to anywhere for a flat monthly fee. In addition, these companies often use a pyramid scheme as their marketing approach.

BEWARE - Many of these companies are operating without authority from the Public Service Commission and you may end up not receiving the service you paid for, losing your deposit, advance payments, or more.

Pyramid scheme companies can be identified through their marketing approach. As a general rule, the sales agent will encourage you to not only purchase the company's services, but to become a sales agent as well. The company will suggest that you can make a lot of money through their multi-level commission plan. While their presentation may appear attractive, it is possible that the company has not been given permission to provide telephone service within Florida. If you are approached by a sales agent, or receive literature advertising a "call anywhere for a flat monthly fee" scheme, be careful.

Florida Law requires that a telephone company must apply for and receive certification from the Florida Public Service Commission before providing long distance service between points located within Florida. In this way the Florida Public Service Commission is able to regulate and monitor the service the company provides to you, the customer.

Uncertificated companies which provide long distance service to points within the state are operating illegally. Your first question regarding a prospective company's service should be "Does your company possess a certificate issued by the Florida Public Service Commission?" If the response to this inquiry is no, we recommend you proceed no further.

This information has been provided to protect consumers. If you have any questions or complaints, please contact the Division of Consumer Affairs at 1-800-342-3552 between 7:45 AM and 4:30 PM, Monday through Friday.

Thank You.

A handwritten signature in cursive script that reads "George B. Hanna".

George B. Hanna
Division of Consumer Affairs

FLETCHER BUILDING • 101 EAST GAINES STREET • TALLAHASSEE, FL 32399-0867

An Affirmative Action/Equal Opportunity Employer

HAPPENINGS

(continued from page 38)

charges whenever a guest disputes them. Few guests do this, however.

Bell Canada Enterprises Inc. has gone and changed their name to BCE Inc. as of January 1. They are the parent of Bell Canada, the nation's largest telephone utility. Let's hope it's a change for the better.

U.S. Sprint still can't seem to get its billing system in order. Customers still report not getting bills or getting bills with months' worth of calls on them. Other customers get warning letters saying they haven't paid their bills when it's actually Sprint that hasn't gotten around to processing them. According to some sources, Sprint has been careful not to send warning letters to big customers, regardless of what their records say. So only the small people are falling victim to that blunder.

And finally, in what is perhaps one of the most unfair moves New York Telephone has made in a while, callers who ask a New York Telephone operator for the location of an exchange are now switched to an information operator, for which there is a charge. For the time being, they will warn you that they're doing this. In the near future, they'll just do it, according to a supervisor. It seems a clear and successful attempt at robbing the consumer, who as usual is kept totally in the dark. For those that wish to avoid falling into this trap, we suggest calling an AT&T operator (dial 00) who will provide the information for the proper cost: nothing.

OSUNY

2600 BBS #1

Available 24 hours a day with a wide range of information on computers, telephones, and hacking.

CALL TODAY!

914-725-4060

THE CENTRAL OFFICE

A full range of telephone, radio, computer, and satellite info plus a whole lot more!

2600 BBS #2

914-234-3260

2600 Marketplace

WOULD YOU LIKE TO MAKE SOME MONEY? Big money? Send a business sized S.A.S.E. to: J. Duffy, 408 Michell St., Ridley Park, PA 19078. This plan is completely LEGAL.

FOR SALE: Schematics for red, green, blue and many others. Please write for info to James Surma, 4135 Highland Drive, Mugadore, OH 44260.

QUALITY TAP REPRINTS. Complete set (#1-91) punched and bound. High quality copies with all special supplementals. \$75/set, shipped UPS or USPS or \$90/set shipped Federal Express. Money orders only,

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

WANTED: G- "Better Homes and Blueboxing Part 2" by Mark

Tabas. If anyone can provide a hard-copy, please send it to JRE, 1447 Graber Dr., Cleveland, OH 44107.

TAP BACK ISSUES, complete set Vol. 1-90 of QUALITY copies from originals. Includes schematics and indexes. \$100 postpaid via UPS or First Class Mail. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

8038 CHIP WITH SPEC SHEET, block diagram and pinout--very limited quan. \$15.00 each postpaid, checks, m.o. to P.E.I., cash, m.o. shipped same day, checks must clear. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

WANTED: Any hacker and phreaker

software for IBM compatible and Hayes compatible modem. If you are selling or know anyone who is, send replies to Mark H., P.O. Box 7052, Port Huron, MI 48301-7052.

FOR SALE: Okidata Microline 92 personal printer. Includes manual for instructions. Hardly used. Make an offer and if it's reasonable, I will pay postage. Matt Kelly, 310 Isbell, Howell, MI 48843.

BLUE BOXING? Let's exchange info on phone numbers, parts, and etc. Write to: Blue Box, P.O. Box 117003, Burlingame, CA 94011, Attention D.C.

FOR SALE: 8038 multi-purpose tone generator chips, prime quality \$7.50 each ppd. Includes comprehensive applications

data. Two chips will generate any dual tone format. These are no longer in production. Get 'em while they last. Bruce, P.O. Box 888, Stinson Beach, CA 94970.

FOR SALE: Radio Shack CPA-1000 Pen Register. Just like new. \$70.00. J.C. Devendorf, 29261 Buckhaven, Laguna Niguel, CA 92677-1618.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info.

Deadline for Summer issue: 5/31/88.

AT&T/BOC

The following is a list of routing codes used by AT&T and Bell Operating Companies (BOC) that you can blue box to. Most codes are used by dialing KP+NPA+XXX+ST, where XXX= the code, except where noted. There are notes attached after this list. Codes marked with a ? are unfamiliar to us.

- 000 Rate Quote System (RQS) (1)
- 001-005 Spare (2)
- 006-008 Reserved (3)
- 009 RQS
- 010 Reserved
- 011 International Origination Toll Center (IOTC) (15)
- 014 TWX Switching Plan (Canada) (?)
- 015-071 Spare
- 072-079 Reserved
- 080-081 Spare
- 082-087 Reserved
- 088 Spare
- 089 Reserved
- 090-099 Spare
- 100 Plant Test- balance termination
- 101 Plant Test- test board
- 102 Plant Test- Milliwatt tone (1004 htz)
- 103 Plant Test- signaling test termination
- 104 Plant Test- 2-way transmission and noise test
- 105 Plant Test- Automatic Transmission Measuring System/Remote Office
Test Line (ROTL)
- 106 Plant Test- CCSA loop transmission test
- 107 Plant Test- par meter generator
- 108 Plant Test- CCSA loop echo support maintenance
- 109 Plant Test- echo canceler test line
- 110-119 Operator Codes
 - 115 Operator Leave Word
 - 116 Inward DA
- 120 Network Emergency Center (?)
- 121 Inward Operator (9)
- 122 AT&T Readyline INWATS (4)
- 123-130 Reserved
- 131 Directory Assistance
- 132-137 Reserved
- 138 IDDD for Equal Access (7)
- 139-140 Reserved
- 141 Rate and Route (10)
- 142-147 Reserved
- 148 Points not on an NPA- Hermosillo, Mexico (5)
- 149 Reserved
- 150 Cable Control (Satellite Avoidance)- Hawaii (5)
- 151 International Assistance
- 152-157 Reserved
- 158 Operator Assistance for Equal Access (7)
- 160 International Operator Center (IOC) (6)
- 161 Trunk Trouble Reporting
- 162-167 Reserved
- 168 Points not on an NPA- Grenada
- 169-170 Reserved
- 171 Points not on an NPA- Monterey, Mexico
- 172 Points not on an NPA- Dominican Republic, Puerto Rico, Virgin

ROUTING CODES

Islands. (Canada Only)

- 173 Reserved
- 174 Cable Control (Satellite Avoidance)- Caribbean
- 175 Reserved
- 176 Points not on an NPA- Mexicali, Mexico
- 177-178 Reserved
- 179 Points not on an NPA- Grenada
- 180 Points not on an NPA- Mexico Numbers
- 181 Toll Station
- 182 International Switching Center (ISC) White Plains, 5 (14)
- 183 ISC New York, BW24
- 184 ISC Pittsburgh
- 185 ISC Atlanta 01T
- 186 ISC Sacramento
- 187 ISC Denver\Sherman Oaks? (15)
- 188 ISC New York, 5450
- 189 Points not on an NPA- Mexico City, Mexico
- 190 Points not on an NPA- Mexico Numbers
- 191 Conference loop around
- 191 AT&T Advanced 800 Intercept recording frames (4)
- 192 Reserved
- 193 Cable Control (Satellite Avoidance)- Grenada
- 194 Points not on an NPA- Tijuana, Mexico
- 195 AT&T Advanced 800 (4)
- 196 AT&T International 800 (4)
- 197 Reserved
- 198 AT&T International City Service Center (ICSC)
- 199 Cable Control (Satellite Avoidance)- Alaska
- 199 AT&T USA Direct (4)

4 or 5 digit codes (8)

- 1150,11501 Universal or Coin Callback
- 1151,11511 Conference Operator (11)
- 1152,11521 Mobile Service/Air Ground
- 1153,11531 Marine Service (12)
- 1154,11541 Toll Terminal
- 1155,11551 Time and Charges callback
- 1156,11561 Hotel/Hotel callback
- 1157,11571 IOTC access trunk
- 1158,11581 Inward- completion assistance (BOC)
- 1159,11591 Inward- Busy Line Verification (BOC)
- 1160,11601 Calling Card Validation- dial pulse equipment (13)
- 1161,11611 Calling Card Validation- DTMF equipment
- 1162,11621 Calling Card Validation- multifrequency (MF) equipment

NOTES:

(1) The Rate Quote System is a voice response system used by operators to obtain routing information. The system, now being phased out, was used as an alternative to calling the Rate & Route operator. Operators would key-in required routing information and a synthesized voice would respond. Though the RQS is still operational, operators now obtain routing information from COMPIS (see note 10).

(continued on next page)

(continued from previous page)

To place a call to the RQS first dial:
KP+NPA+XXX+ST where XXX= the RQS routing code. After a wink (short burst of 2600 hz), dial in MF one of the following:

KP+00+ONPA+NXX+TNPA+NXX+ST to get the "rate step" for the current time of day.

KP+01+ONPA+NXX+TNPA+NXX+ST to get the rate step for a day (8am-5pm) call.

KP+02+ONPA+NXX+TNPA+NXX+ST for the rate step of an evening(5pm-11pm) call.

KP+03+ONPA+NXX+TNPA+NXX+ST for the rate step of a night(11pm-8am) call.

KP+04+? We are not familiar with how to use this feature, it has to do with calls to Mexico.

KP+05+NPA+NXX+ST gives the routing for a Bell Operating Company (BOC) inward (see note 9).

KP+06+NPA+NXX+ST gives the routing for an AT&T inward operator (see note 9).

KP+07+XXXXXXXX+ST gives a tone check and reads off the numbers you just dialed.

KP+08+? is used with Enterprise and Zenith numbers. We are not familiar with this function.

KP+09+NPA+NXX+ST gives you the current time for the area code and exchange you dialed.

(2) When a code is marked spare, that means that there is no current or planned networkwide usage. It still may be utilized as a non-standard POTS exchange for WATS service by local companies.

(3) When a code is marked reserved it means that there may be planned networkwide usage.

(4) This code is used by an AT&T custom service. It may be thought of as acting like a special area code and takes the following dialing format: KP+XXX+yyy+yyyy+ST where XXX-is the code in question and y can be any number (0-9).

(5) All "Points not on an NPA" and "Cable Control" function as pseudo area codes and are followed by a telephone number.

(6) Calls to the IOC are dialed as follows KP+160+CCC+ST CCC=The country code (i.e. 044 or 144 for the UK). For ship calls via Marisat you dial as follows: Atlantic 160+871, Pacific 160+872, and Indian 160+873.

ROUTING CODES

(7) These are special codes used to with equal access. They are as follows:

KP+138+PIC+ST then KP+CC+cc+xxxxx+ST
KP+158+PIC+ST

where PIC= is the Primary Carrier code (i.e., 333 for US Sprint, 222 for MCI). CC= Country code cc=city code and xxxxx= number. We're not sure exactly when and where these are used.

(8) All 4 and 5 digit codes are dialed as follows: KP+NPA+XXXX+ST or KP+NPA+XXXXX+ST. Keep in mind that not every code is in use in every NPA.

(9) The format for an AT&T inward is usually KP+NPA+121+ST--in some small cities there is an extra code used called a Terminating Toll Center (TTC) or sometimes just a city code. If a TTC is used the format is KP+NPA+TTC+121+ST. To get an inward with most BOCs you dial KP+NPA+11591+ST but there are some which use a format of KP+NPA+TTC+121+ST. To get the inward routing for a particular exchange, use the Rate Quote System.

(10) The number for Rate and Route was 800+141+1212 but this was discontinued sometime last year, when the TSPS operators got a computer terminal called COMPIS. In each state there is an inward which acts like a Rate and Route operator. In New York it's 716+121.

(11) With the advent of Alliance Teleconferencing, use of the conference operator dwindled. There are currently 4 operator centers handling conferences. They are as follows: Atlanta 404+11511, Minneapolis 507+11511, New York 212+11511, and Oakland 415+11511. 800-225-0233 translates to the conference operator closest to you.

(12) The marine operator is used in calling ships that are close to the United States. There is an operator called the "High Seas" operator who can be reached by dialing 800-SEA CALL (800 732 2255). The High Seas operator is a service of AT&T, while Marisat is an independent company (see note 6). A High Seas call can go to any ocean for 14.98 for the first 3 minutes and 4.98 for each additional minute. A Marisat only calls to 3 oceans and costs 10 dollars a minute.

(13) 116X and 116XX are used to verify an AT&T calling card number. You dial KP+NPA+116XX+ST when you hear a "long" you dial the calling card number. If you use 11611 you enter the number in touch tone and if you use 11621 you enter the card number in MF using KP and ST.

(14) These ISC codes are used to provide alternate routing for electro mechanical switches. Some older electro-mechanical switches, for example the #5 Cross-Bar (5XB) cannot outpulse 011+CCC (CCC-

(continued on next page)

AT&T/BOC ROUTING CODES

(continued from previous page)

country code) for international dialing. AT&T has set up these special codes to handle international calls. A 5XB can dial KP+18X+ST. They would then receive a wink (short blast of 2600 hz) and would proceed to dial the country code and number. If you want to make an international call you dial KP+(NPA)+18X+ST where the NPA is optional. After the wink dial the country code, city code, and number. The comma "," after the city name is the switch number if there is more than one 4ESS in that city.

(15) The 187 code was assigned to Atlanta until up to the end of February. AT&T is in the process in routing the calls to the Sherman Oaks office in California.

(16) To make international calls dial KP+011+CCC+ST where CCC=the country code; and then dial KP+CC+XXXXXX+ST where CC=city code and XXXXXX= the telephone number. Also see notes 5, 6, 7, 12, 14, and 15.

The USSR has been off direct dial for many years and due to this fact there is not much information available about its telephone network. The country code for the USSR is 007 and some city codes are: Kiev 0442, Leningrad 812, Minsk 172, and Moscow 095. The only number which can be dialed direct from the US is 007-095-2522457 which is the US embassy in Moscow. ALL other numbers must be dialed by the Moscow operator. Even the embassy must be dialed by the ICO (International Operator Center).

In July 87, we ran an article (How Phreaks are Caught) which included the 800 number allocation for long distance carriers. This is an updated list of the 800 exchanges that route directly to US Sprint: 800-326, 800-347, 800-359, 800-366, 800-546, 800-669, 800-726, 800-729, 800-733, 800-735, 800-736, 800-767, 800-776, 800-827, 800-877.

If you have any interesting numbers, scan sheets, NUA's, or anything similar send to:

2600
PO BOX 99
Middle Island, NY 11953-0099

1986

PRIVATE SECTOR RETURNING—Back online soon but many questions on seizure remain, THE BASICS DIVESTITURE: WHAT HAPPENED?—an explanation of that which is confusing the populace, FLASH AT&T steals customers, Dominican blue boxers, computerized hooky catcher, Falwell attacked by computer, an astronomical phone bill, dial-a-porn update, phone booth victorious, LETTERS Getting credit from alternate carriers, tracing methods, mobile phones, Manitoba raid, 2600 INFORMATION BUREAU—blue box programs; SYSTEMATICALLY SPEAKING confusing payphones, code abuse software, centrex features in your house, VAX 8650, overcharge hunters; VMS THE SERIES CONTINUES—more on security features, IT COULD HAPPEN TO YOU!—what happens when hackers have a fight, DIAL BACK SECURITY—holes in the systems, FLASH abuse of party line, unique obscene caller, news on pen registers, reporters steal Swiss phones, pay phone causes panic; LETTERS asking questions, blue box corrections, Computel complaint, BBS security, 2600 INFORMATION BUREAU—assorted numbers, SYSTEMATICALLY SPEAKING Sprint and US Tel merge, write protect tabs wrong, Bell Atlantic chooses MCI, cellular phones in England, infrared beeper, electronic tax returns, acoustic trauma, AN OVERVIEW OF AUTOVON AND SILVER BOXES—the military phone network and how your touch tone phone can play along AN AMERICAN EXPRESS PHONE STORY—a memory of one of the better hacking escapades, FINAL WORDS ON VMS—security devices and assorted tips, FLASH hacker zaps computer marquee, Soviets denied computer access, calling the shuttle, new ways of stealing data, computer password forgotten, LETTERS corporate rates, defeating call waiting, ringback numbers, where is BIOC?, credit where it's due, special 800 number, THIS MONTH AT 2600: Private Sector's return, Computel and Compuserve, Telepub '86, a postal miracle, SYSTEMATICALLY SPEAKING Jamming satellites, TASS news service, Soviet computer update, dialing the yellow pages, Northern Telecom to destroy CO's, more phones than ever, RSTS FOR BEGINNERS—basic system functions, login procedures; MOBILE PHONES THEORY AND CONSTRUCTION—how to build your own mobile phone, FLASH, British phonebooth wedding, another large Sprint bill, bad tenant databases, car breathalizers, phone phreak fined, Marcos phones for free; LETTERS blue box coding, electronic road pricing in Hong Kong, UNIX bugs, more on AE hacking, A STORY OF EAVESDROPPING—from World War II, THIS MONTH AT 2600 transcripts of Private Sector raid, more on Computel, SYSTEMATICALLY SPEAKING '617 to be divided, Congress chooses AT&T, Baby Bells don't pay AT&T bills, equal access 800 numbers, data encryption, DA failure, AT&T loses its zero, EXPLOITS IN OPERATOR HELL—harassing operators from Alaska, THE COMPUTEL SCOOP, FLASH Bellcore publications go public, US and France link phones, computer grammar, shower phone, cellular modem, high tech parking meters, Congressional computer, LETTERS foreign phone systems, Russian phone books, numbers to dial on a blue box, Boston ANI, Cheshire Catalyst, CNA, ways of answering the phone, 2600 INFORMATION BUREAU—Autovon numbers, alternate phreaking methods for alternate carriers, SYSTEMATICALLY SPEAKING Wrestlemania pins Bell, sting boards on the rise, American Network fears hackers, free pay-phones plague New Jersey, disposable phones, hacker terrorists, COMPUTER CRIME REVIEW—a review of the report from The National Center for Computer Crime Data, HOW TO HACK A PICK—An introduction to the Pick operating system and ways of hacking into it, NOTHING NEW IN COMPUTER UNDERGROUND—review of a new book, FLASH New York's new computer crime law, a \$6,829 phone bill, how big computer crime pays, public phone secrecy, Capitol Hill hacker, Citibank money games, LETTERS English phreaking, ways of tricking sting BBS's, called party supervision, 2600 Phun Book, Captain Midnight, RCI, 2600 INFORMATION BUREAU—some phone numbers, RESOURCES GUIDE, SYSTEMATICALLY SPEAKING Hands across Telenet, calling Kiev, Nynex bumps off Southwestern Bell, stock market crash, cell site names, videophones, VIOLATING A VAX—Trojan horses, collecting passwords, etc., etc., THE FREE PHONES OF PHILLY—Skyline providing completely free service from pay phones, FLASH town crippled by telco strike, prisoners make illegal calls, hacker degrees, New Jersey tops taps, ex fed is tapped, water company wants customers' social security numbers, computers strike again, federal employees "tracked", LETTERS Association of Clandestine Radio Enthusiasts, ITT correction, NSA, more on VMS, Telecomputist, a 950 trick, 2600 INFORMATION BUREAU—World Numbering Zones, SYSTEMATICALLY SPEAKING AT&T selling payphones, automated operators, cellular dial-by-voice, new British phone service, no data protection for Hong Kong, Congressional fraud hotline, federal phone failures, Indiana telco threatens AT&T, KNOWING UNIX—sending mail and general hacking, A TRIP TO ENGLAND—and the fun things you can do with phones over there, FLASH Phone fraud in governor's house, Big Brother, Teltec fights back, vandalism, 911 calls, LETTERS shutting down systems, legal BBS's, VAX, VMS tips, 2600 INFORMATION BUREAU—a list of telcos, a list of area codes and number of exchanges; SYSTEMATICALLY SPEAKING USSR computers, ATM's in China, NYCE, TV blue boxes, government phones, rural radio phones, SOME FACTS ON SUPERVISION—answer supervision explained, RCI & DMS-100 BUGS, ANOTHER STINGER IS STUNG—Maxfield exposed again, FLASH, NSA drops DES, hackers on shortwave, Big Brother traffic cop, crosstalk saves a life, Indian phones, video signatures, FBI shopping list, airphone causes confusion, LETTERS Captain Midnight, annoyance bureau, SL-1 switches, credit, PBX's, 800 word-numbers, public CNA's; 2600 INFORMATION BUREAU—Winnipeg numbers, SYSTEMATICALLY SPEAKING Sprint overbills, AT&T ranks #1, portable VAXes, call rejection, DEATH OF A PAY PHONE—nasty business, TRASHING AMERICA'S SOURCE FOR INFORMATION—still more tactics, FLASH FBI investigates coffee machine, CIS copyrights public software, Navy software, HBO encryption, Indiana "Fones", LETTERS Numbers, telco harassment, Puerto Rican telephones, Q's and Z's, 2600 INFORMATION BUREAU—Overseas numbers, SYSTEMATICALLY SPEAKING Electronic tax returns, software makers crash BBS, ICN, Ultraphone, ESS in Taiwan, NSA wants new chip, ICN—MORE THAN A BARGAIN—a look at one of the worst phone companies in the world, MASTERING THE NETWORKS—communicating on Arpanet, Bitnet, etc., FLASH Reagan tortures patients, FBI angers parents, Q and Z controversy, LETTERS Telenet hacking, ANI's, 811, 976 problems, 2600 INFORMATION BUREAU—British BBS numbers, WRATH OF GOD STRIKES 2600, SYSTEMATICALLY SPEAKING Banks link arms, Sprint has too many customers, new payphones, nickname listings, computer college, A LOCK AT THE FUTURE PHREAKING WORLD—Cellular telephones & how they work, HOW CELLULAR PHONES CAME ABOUT AND WHAT YOU CAN EXPECT, THINGS WE'RE NOT SUPPOSED TO KNOW ABOUT, FLASH Avoiding rejection, phreaks tie up circuits, North Carolina hackers, international hacking, paying for touch tones, wiretaps, LETTERS Equal access 800 numbers, strange numbers, Irish phreaking, disabling call waiting, 2600 INFORMATION BUREAU—Netmailsites, SYSTEMATICALLY SPEAKING Free directories, fingerprint ID system, navigating with CD's, sweeping for bugs.

1987 ISSUES ALSO AVAILABLE!



All issues now in stock. Delivery within 4 weeks.
MAKE YOUR COLLECTION COMPLETE!

2600 BACK ISSUE ORDER:

1984 \$25 1985 \$25 1986 \$25 1987 \$25

SEND THIS COUPON WITH PAYMENT TO:

2600 Back Issues

P.O. Box 752

Middle Island, NY 11953

(your address label should be on the back of this form)

CONTENTS

MONITORING PHONE CALLS	4
MORE ON VM/CMS	9
WEATHERTRAK CODES	15
THE HACKER THREAT	16
PRIVATE SECTOR SCAM REVISITED	21
LETTERS	24
A ROLM CATASTROPHE.....	30
HAPPENINGS.....	37
2600 MARKETPLACE	41
AT&T/BOC ROUTING CODES.....	42

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

SECOND CLASS POSTAGE
Permit Pending at
East Setauket, N.Y.
11733
ISSN 0749-3851

**DANGER:
MISSING LABEL**

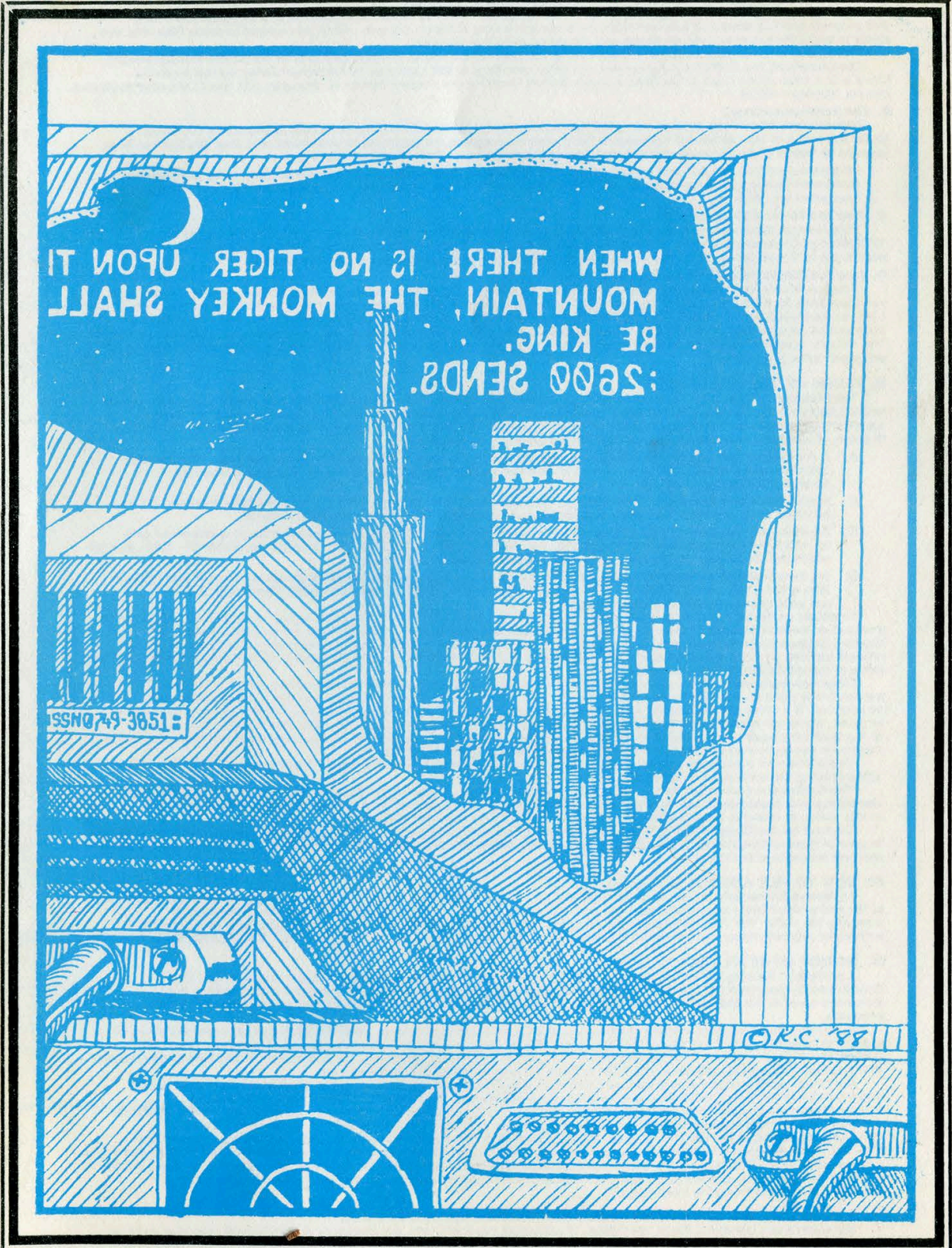
2600



The Hacker Quarterly

Volume 5, Number 2

Summer, 1988



IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN RE LONG DISTANCE
TELECOMMUNICATIONS LITIGATION

MDL Docket No. 598
All Cases
Hon. Anna Diggs Taylor

**NOTICE OF CLASS ACTION AND PROPOSED SETTLEMENT TO CERTAIN CURRENT AND
FORMER CUSTOMERS OF ALLNET COMMUNICATION SERVICES, INC.**

By Order of the United States District Court for the Eastern District of Michigan, PLEASE TAKE NOTICE THAT:
A class action lawsuit has been filed on behalf of certain former and current customers against Allnet Communication Services, Inc., formerly known as Combined Network, Inc. The Court has preliminarily approved a settlement of this lawsuit.
YOU ARE URGED TO READ THIS NOTICE CAREFULLY BECAUSE IT AFFECTS YOUR RIGHTS AND WILL BE BINDING ON YOU IN THE FUTURE.

I. NOTICE OF A PENDING CLASS ACTION

A. Description of the Lawsuit

Plaintiffs have sued Allnet, alleging that Allnet charged customers for certain unanswered telephone calls, holding time, busy signals, and central office recordings (collectively "unanswered calls") without adequately disclosing such charges to their customers or the public. Plaintiffs seek to present their own claims for charges for unanswered calls, as well as the claims of other current and former Allnet customers for similar charges.

Allnet denies the violations alleged by plaintiffs and contends that at all times Allnet has charged its subscribers fairly and properly and has disclosed fully and fairly the basis for its long distance charges. Allnet has agreed to settle Plaintiffs' suit solely to avoid the expense, inconvenience and disruption of further litigation.

This Notice is not an expression of any opinion by the Court of the merits of this litigation or of the Settlement Agreement. The Complaint, the Settlement Agreement and other pleadings in this case may be inspected during normal business hours at the office of the Clerk of the United States District Court for the Eastern District of Michigan, 231 West Lafayette Boulevard, Detroit, Michigan 48226.

B. The Settlement Class.

Plaintiffs and Allnet have entered into a Settlement Agreement, which has been preliminarily approved by the Court. Under the terms of the Settlement Agreement, the parties have agreed, for purposes of settlement only, that this suit has been brought on behalf of the following class of persons similarly situated to Plaintiffs (the "Class"):

All persons and entities that subscribed to and utilized the long distance telephone service of Allnet or its predecessor, Combined Network, Inc. (referred to collectively as "Allnet"), at any time during the period March 2, 1981 through December 31, 1985.

C. How to Remain a Class Member.

If you were a subscriber to and utilized Allnet's long distance telephone service at any time during the period March 2, 1981 through December 31, 1985, you are a member of the Class. If you choose to remain a member of the Class, you may participate in this settlement and you will be bound by the results of the settlement and/or the lawsuit.

D. How to Exclude Yourself From the Class.

You are not required to be a member of the Class. Should you decide that you do not want to be a member of the Class, you must send an exclusion notice that states your name, current address, and your desire to be excluded from the Class to the Clerk of the United States District Court for the Eastern District of Michigan at the address given at the end of this Notice, postmarked no later than June 18, 1988. If you choose to be excluded from the Class, you may not participate in the settlement. You will not, however, be bound by any judgment dismissing this action and you will remain free to pursue on your own behalf any legal rights you may have.

II. TERMS OF THE SETTLEMENT

The Settlement Agreement requires Allnet to provide to class members long distance telephone credits up to a maximum of \$525,000 (the "Settlement Credits") and cash refunds up to a maximum of \$75,000 (the "Cash Refunds"). These benefits are available to Class members who properly complete and file a Proof of Claim in the manner described in Section III below. Class members may choose one benefit from the following options:

- A. A *standardized credit* toward Allnet long distance telephone service of 90 cents for each year from 1981 through 1985 in which the Class member: (i) was an Allnet customer; and (ii) claims that she/he was charged by Allnet for unanswered calls; or
- B. A *standardized cash refund* of 90 cents for each year from 1981 through 1985 in which the Class member: (i) was an Allnet customer; and (ii) claims that she/he was charged by Allnet for unanswered calls; or
- C. An *itemized credit* toward Allnet long distance telephone service of 30 cents for each minute of unanswered calls for which the Class member was charged during the Class Period (March 2, 1981 through December 31, 1985) and for which the Class member has not been previously reimbursed or credited; or
- D. An *itemized cash refund* of 30 cents for each minute of unanswered calls for which the Class member was charged during the Class period (March 2, 1981 through December 31, 1985) and for which the Class member has not been previously reimbursed or credited.

To obtain an *itemized credit* or cash refund, the Class member must itemize and attest to each unanswered call for which a refund or credit is claimed. If the total credits claimed by Class members exceed \$525,000, each Class member claiming Settlement Credits will receive his/her/its *pro rata* share of the total Settlement Credits available. If the total cash refunds claimed by Class members exceed \$75,000, each Class member claiming a Cash Refund will receive his/her/its *pro rata* share of the total Cash Refunds available.

Class members need not be current Allnet customers to claim the standardized and itemized credits. Allnet will automatically open an account for any Class member who requests credits and executes an authorization to open such an account. If a Class member incurs a local telephone company service charge in connection with the opening of an Allnet account, Allnet will issue a credit to the Class member's account for the full amount of such service charge upon receipt of the local telephone company's bill for the service charge. Allnet is not responsible for any other service charge that a local telephone company may impose for ordering, using or terminating Allnet service.

The Settlement Agreement requires Allnet to pay the costs of giving this Notice (up to a maximum of \$240,000) and of administering the settlement described above.

The Settlement Agreement further provides that upon final approval of the settlement, the Court will enter a judgment dismissing with prejudice all claims of plaintiffs and members of the Class that have been or might have been asserted in this action or relate to Allnet's billing and disclosure practices for unanswered calls.

Counsel for the Class have investigated the facts and circumstances regarding the claims against Allnet and their defenses. In view of those circumstances, counsel for the Class have concluded that this Settlement Agreement is fair and reasonable and in the best interests of the Class.

III. HOW TO FILE A PROOF OF CLAIM

To receive Settlement Credits or a Cash Refund, you must provide all of the information requested in the Proof of Claim at the end of this Notice and return it to the Clerk of the Court at the address indicated below, postmarked no later than July 28, 1988. The Proof of Claim must be signed by the Class member or, if the Class member is not an individual, an authorized representative. All claims are subject to confirmation and approval. PLEASE FILL OUT THE CLAIM FORM CAREFULLY.

IV. NOTICE OF SETTLEMENT HEARING

A settlement hearing will be held on June 28, 1988 before the Honorable Judge Anna Diggs Taylor, United States Courthouse, in Courtroom 737 at 231 West Lafayette Boulevard, Detroit, Michigan. The purpose of the hearing is to determine whether the Settlement Agreement should be approved and confirmed by the Court as fair, reasonable, and adequate.

At the settlement hearing, counsel for the Class shall petition the Court for an award of attorneys' fees and expenses not to exceed \$100,000. Allnet has agreed not to oppose this petition. In addition, Allnet has agreed to reimburse plaintiffs' counsel for up to an additional \$15,000 for fees and expenses incurred in monitoring the settlement. These fees and expenses shall not reduce any of the Settlement Credits or Cash Refunds available to Class members.

Any Class member wishing to appear and be heard at the Settlement Hearing must file a notice of intention to appear with the Clerk of the Court, which notice must be postmarked no later than June 18, 1988. If such Class member objects to any one or more terms of the Settlement Agreement, the notice of intention to appear must be accompanied by a statement of the basis for this objection. A Class member may also object to the Settlement Agreement without personally appearing at the hearing by filing written objections to the Settlement with the Clerk of the Court no later than June 18, 1988. A copy of the objections in any case must also be served upon lead counsel for the plaintiff class, Sachnoff Weaver & Rubenstein, Ltd., Attention: Allnet Settlement, 30 South Wacker Drive, Suite 2900, Chicago, Illinois 60606. You will not be heard at the hearing or entitled to contest the Proposed Settlement unless you file and serve your objections in accordance with the foregoing instructions.

V. IF YOU HAVE ANY QUESTIONS ABOUT THIS NOTICE OR THIS LAWSUIT

If you have any questions about this Notice, the attached Proof of Claim, the lawsuit or the Settlement, you may write to: Allnet Settlement, P. O. Box 277, Franklin, Michigan 48025.

NO TELEPHONE CALLS CONCERNING THIS NOTICE SHOULD BE MADE TO ALLNET, COUNSEL FOR PLAINTIFFS, OR THE COURT.

(continued on page 42)

We think you'll find this issue to be most informative and educational. At last we've devoted some space to the subject of computer viruses.

But we've done it in a way no other magazine has yet done. For the first time, you can read what goes through the mind of someone who deliberately plants viruses in computer systems. And you can also see what measures are being taken to thwart this person's efforts.

We're happy to announce yet

another 2600 computer bulletin board, this one in the Washington DC area. This one is PC-Pursuitable and you can reach it at (703) 823-6591. Hopefully, we'll expand to the west coast by next issue.

Remember that 2600 meetings now take place on the first Friday of the month only. See page 41 for details. Turnout has been quite good in recent months.

STAFFBOX

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Bobby Arwatt

Production
Mike DeVoursney

Cover Art
Ken Copel

Writers: Eric Corley, John Drake, Mr. French, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOC, David Ruderman, Bernie S., Silent Switchman, Mike Yuhás, and the usual anonymous bunch.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright © 1988, 2600 Enterprises Inc.

Yearly subscription: U.S. and Canada—\$15 individual, \$40 corporate.

Overseas—\$25 individual, \$55 corporate.

Back issues available for 1984, 1985, 1986, 1987 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.

2600 Office Line: 516-751-2600

BBS #1 (OSUNY): 914-725-4060

BBS #2 (CENTRAL OFFICE): 914-234-3260

BBS #3 (YOYODYNE): 402-564-4518

BBS #4 (BEEHIVE): 703-823-6591

USENET ADDRESS: 2600@dasys1.UUCP

ARPANET ADDRESS: phri!dasys1!2600@nyu

A Form of Protection

by Ross M. Greenberg

What is a Trojan?

Back in the good old days (before there were computers), there was this bunch of soldiers who had no chance of beating a superior force or of even making it into their fortress. They had this nifty idea: present the other side with a gift. Once the gift had been accepted, soldiers hiding within the gift would sneak out and overtake the enemy from within.

We can only think of the intellectual giants of the day who would accept a gift large enough to house enemy soldiers without checking its contents. Obviously, they had little opportunity to watch old World War II movies to see the same device used over and over again.

Consider the types of people who would be thrilled at the concept of owning their own rough hewn, large wooden horse! Perhaps they wanted to be the first one on their block, or something silly like that.

Anyway, you're all aware of the story of The Trojan Horse.

Bringing ourselves a bit closer to the reality we've all grown to know and love, there's a modern day equivalent: getting a gift from your BBS or user group which contains a little gem which will attack your hard disk, destroying whatever data it contains.

In order to understand how a potentially useful program can cause such damage when corrupted by some misguided soul, it's useful to understand how your disk works, and how absurdly easy it is to cause damage to the data contained thereon. So, a brief technical discussion of

the operation of your disk is in order. For those who aren't concerned, turn the page or something.

Data is preserved on a disk in a variety of different physical ways having to do with how the data is encoding in the actual recording of that data. The actual *structure* of that data, however, is the same between MS-DOS machines. Other operating systems have a different structure, but that doesn't concern us now.

Each disk has a number of "tracks". These are sometimes called cylinders from the old type IBMers. These are the same people who call hard disks DASDs (Direct Access Storage Devices), so we can safely ignore their techno-speak, and just call them tracks. Tracks can be thought of as the individual little grooves on an audio record, sort of.

Anyway, each track is subdivided into a number of sectors. Each track has the same number of sectors. Tracks are numbered, as are sectors. Any given area on

"Typical Trojan programs cause damage to your data, and were designed to do so by the worms who writhe in delight at causing this damage."

the disk can be accessed if a request is made to read or write data into or out of Track-X, Sector Y. The read or write command is given to the disk controller, which is an interface between the computer itself and the hard disk. The controller figures

For You and Your Computer

out what commands to send to the hard disk, the hard disk responds and the data is read or written as directed.

The first track on the hard disk typically will contain a small program which is read from the hard disk and executed when you first power up your machine. The power up sequence is called "booting" your machine, and therefore the first track is known as the "boot track".

In order to read information from your disk in a logical sequence, there has to be some sort of index. An unusual index method was selected for MS-DOS. Imagine going to the card index in a library, looking up the title you desire, and getting a place in another index which tells you where on the racks the book is stored. Now, when you read the book, you discover that only the first chapter of the book is there. In order to find the next chapter of the book, you have to go back to that middle index, which tells you where the next chapter is stored. This process continues until you get to the end of the book.

Sounds pretty convoluted, right? You bet! However, this is pretty much how MS-DOS does its "cataloguing" of files.

The directory structure of MS-DOS allows for you to look up an item called the "first cluster". A cluster represents a set of contiguous ("touching or in contact" according to Random House) tracks and sectors. It is the smallest amount of information which the file structure of MS-DOS knows how to read or write.

Based on the first cluster number as stored in the directory, the first portion of a file can be read. When the information contained therein is exhausted, MS-DOS goes to that secondary index for a pointer

to the next cluster. That index is called the File Allocation Table, commonly abbreviated to "FAT". The FAT contains an entry for each cluster on the disk. An FAT entry can have a few values: ones which indicate that the cluster is unused, another which indicates that the associated cluster has been damaged somehow and that it should be marked as a "bad cluster", and a pointer to the next cluster for a given file. This allows for what is called a linked list: once you start looking up clusters associated with a given file, each FAT entry tells you what the next cluster is. At the end of the linked list is a special indicator which indicates that there are no more clusters associated with the file.

There are actually two copies of the FAT stored on your disk, but no one really knows what the second copy was intended for. Often, if the first copy of the FAT is corrupted for some reason, a clever programmer could recover information from the second copy to restore to the primary FAT. These clever programmers can be called "hackers", and should not be confused with the thieves who break into computer systems and steal things, or the "worms" [Joanne Dow gets credit for *that* phrase!] who would get joy out of causing you heartache!

But that heartache is exactly what can happen if the directory (which contains the pointer to the first cluster a file uses), the FAT (which contains that linked list to other areas on the disk which the file uses), or other areas of the disk get corrupted.

And that's what the little worms who create Trojan programs do: they cause what at first appears to be a useful pro-

(continued on next page)

Protecting Yourself

gram to eventually corrupt the important parts of your disk. This can be as simple as changing a few bytes of data, or can include wiping entire tracks clean.

Not all programs which write to your hard disk are bad ones, obviously. Your word processor, spreadsheet, database, and utility programs have to write to the hard disk. Some of the DOS programs (such as FORMAT), if used improperly, can also erase portions of your hard disk causing you massive amounts of grief. You'd be surprised what damage the simple "DEL" command can do with just a simple typo.

But what defines a Trojan program is its delivery mechanism: the fact that you're running something you didn't expect. Typical Trojan programs cause damage to your data, and were designed to do so by the worms who writhe in delight at causing this damage. May they rot in hell -- a mind is a terrible thing to waste!

Considering the personality required to cause such damage, you can rest assured that they have few friends, and even their mother doesn't like to be in the same room with them. They sit back and chortle about the damage they do with a few other lowly worms. This is their entire social universe. You should pity them. I know that I do.

What is a Virus?

Trojan programs are but a delivery mechanism, as stated above. They can be implemented in a clever manner, so that they only trigger the malicious part on a certain date, when your disk contains certain information or whatever. However they're coded, though, they typically affect the disk only in a destructive manner once triggered.

A new breed of programs has the capability of not only reserving malicious damage for a given event's occurrence, but of also replicating itself as well.

This is what people refer to when they mention the term "Virus Program".

Typically, a virus will spread itself by replicating a portion of itself onto another program. Later, when that normally safe program is run it will, in part, execute a set of instructions which will infect other programs and then potentially, trigger the Trojan portion of the program contained within the virus.

The danger of the virus program is twofold. First, it contains a Trojan which will cause damage to your hard disk. The second danger is the reason why everyone is busy building bomb shelters. This danger is that the virus program will infect other programs and they in turn will infect other programs and so forth. Since it can also infect programs on your floppy disks, you could unknowingly infect other machines! Pretty dangerous stuff, all right!

Kenneth van Wyck, one of the computer folks over at Lehigh University, first brought a particular virus to the attention of the computer community. This virus infects a program, which every MS-DOS computer must have, called COMMAND.COM. This is the Command Line Interpreter and is the interface between your keyboard and the MS-DOS operating system itself. Whatever you type at the C> prompt will be interpreted by it.

Well, the virus subverts this intended function, causing the infection of neighboring COMMAND.COMs before continuing with normal functionality of the command you typed. After a certain number of

From Infection

"infections", the Trojan aspect of the program goes off, causing you to lose data.

The programmer was clever. But still a worm. And still deserving of contempt instead of respect. Think of what good purposes the programmer could have put his or her talents to instead of creating this damage. And consider what this programmer must do, in covering up what they've done. They certainly can't tell anyone what they've accomplished. Justifiable homicide comes to mind, but since the worms they must hang around are probably as disreputable as they are, they must hold their little creation a secret.

A pity. Hopefully, the worm is losing sleep. Or getting a sore neck looking behind them wondering which of their "friends" are gonna turn them in.

The Challenge to the Worm

When I first released a program to try to thwart their demented little efforts, I published this letter. What I say in it still holds:

"As for the designer of the virus program: most likely an impotent adolescent, incapable of normal social relationships, and attempting to prove their own worth to themselves through these types of terrorist attacks.

"Never succeeding in that task (or in any other), since they have no worth, they will one day take a look at themselves and what they've done in their past, and kill themselves in disgust. This is a Good Thing, since it saves the taxpayers' money which normally would be wasted on therapy and treatment of this miscreant.

"If they *really* want a challenge, they'll try to destroy *my* hard disk on my BBS, instead of the disk of some innocent per-

son. I challenge them to upload a virus or other Trojan horse to my BBS that I can't disarm. It is doubtful the challenge will be taken: the profile of such a person prohibits them from attacking those who can fight back. Alas, having a go with this lowlife would be amusing for the five minutes it takes to disarm whatever they invent.

"Go ahead, you good-for-nothing little slimebucket: make *my* day!"

Alas, somebody out there opted to do the cowardly thing and use the FLUSHOT programs as a vehicle for wrecking still more destruction on people like you. The FLUSHOT3 program was redistributed along with a companion program to aid you in reading the documentation. It was renamed FLUSHOT4. And the reader program was turned into a Trojan itself.

(continued on page 28)

From the Guinness Book of World Records:

The largest collection of valid credit cards, as of May 3, 1980, is one of 1,003, all different, by Walter Cavanagh of Santa Clara, CA (known as "Mr. Plastic Fantastic"). The cost of the acquisition was nil, and he keeps them in the world's largest wallet, 250 feet long, weighing 31 pounds, and worth more than \$1,250,000 in credit.

Largest Incorrect Telephone Bill
On August 18, 1975, the landlord of the Blue Bell Inn, Lichfield, Staffordshire, England received a telephone bill for \$4,386,800,000. It was later admitted that this bill contained "an arithmetical error".

the dark side

by The Plague

I'm sure you've heard about computer viruses. But what you were probably fed was misinformation. This article will attempt to de-mystify your perception of the computer virus, give you the facts, as well as teach you how to create your very own virus. This is not a second-hand or bystander explanation of viruses; I have had first-hand experience in the writing, distribution, and tracking of my very own virus, so I'm quite knowledgeable on the subject. Most viruses do destroy data. They also spread somewhat exponentially when unnoticed and not controlled. The beauty of the computer virus is that it perfectly mimics a real virus or small organism, thus having the potential of being a great tool in artificial intelligence. I will not write about how to protect yourself from a virus, because that would defeat the purpose of this article, and anyone with common sense already knows how to prevent being infected.

Recently, viruses have been a very hot issue in the media, but I assure you that I'm not jumping on the bandwagon because my virus has been around long before the term "computer virus" was ever mentioned in the media. The media has a very shallow understanding of what a virus is. Examples of the media's reporting of computer viruses include the article in the February 1, 1988 issue of *Newsweek* written by William D. Marbach and Richard Sandza called "Is your computer infected? Systems fall to silent and contagious killers." Another report appeared on ABC World News Tonight in late February, and I must say that the computer animation was quite good. It showed the virus (a pink

spiny blinking sphere) as it entered the resistors on the motherboard (come on, are these guys for real?). This was followed by a guy who claimed to be the inventor of the virus, which is absolutely bogus, because the computer virus was not invented by any one person. I don't even know why he decided to claim the credit -- it's nothing to be proud of.

My experience with viruses comes from writing CyberAIDS, a virus for the Apple II family of computers. This is the first and only virus for the Apple which operates under ProDOS that I know of. Due to ease of use of the ProDOS MLI (Machine Language Interface), it was incredibly easy to write the virus. This is because I didn't need to deal with the hardware directly, only make a few simple system calls (i.e., read block, write block, open file, close file, etc.). The fact that ProDOS runs on the entire spectrum of the Apple II family also allows my virus to reach the broadest audience available. The ProDOS MLI is very similar to the operating systems of most personal computers, mini-computers, and mainframes. Thus the virus can be adapted to run on any computer, so don't make the same mistake that the Apple community made, that is in thinking that a virus will never appear for their computer. Operating systems with similar calls and characteristics as ProDOS MLI are MS-DOS, Unix, AmigaDOS, Atari's TOS, and Macintosh's OS.

I was asked whether I had any moral feelings about viruses, or whether I thought that they were wrong, or evil, or whatever. My feelings are the following: I don't care one way or the other. If people's

of viruses

data is destroyed, then so be it. If people are stupid enough to accept pirated software, then they deserve to be punished. The fact is that most business PC users will never be infected with a virus unless they download public domain or pirated software. Also, businesses may be affected if someone in the organization decides to infect the system, in which case the destruction is not preventable, because the person doing the infecting would have enjoyed destroying data even if viruses didn't exist. As for people who use their computers for home/entertainment/hobby, they are the ones most susceptible to the virus revolution. They should be wary of software that was not previously tested by others. Nowadays, it's becoming quite dangerous to accept software 'off the street'. I hate to use this expression, but "viruses don't kill data, people kill data". A virus is perfectly harmless unless it is being spread by people willingly/unwillingly. Therefore, people must take the responsibility to protect themselves and others by taking precautions. This will not be discussed in this article.

Creating a virus is by no means a simple project. Anyone who has ever attempted to write a virus, or any cybernetic organism for that matter, will tell you about the difficulties and tribulations involved. If anything, I'm quite upset that most people don't realize what an accomplishment this is. One person even told me, "Hey, anybody could write a virus. The reason I never wrote one is because it's wrong to do so." Well, he was wrong at the time because it is quite difficult to write a virus completely from scratch. But perhaps this article will allow anyone to write a virus by

giving them at least a good start.

My main concern about my project was how to track the spread of the virus, in order to gather data. This data could be used in the future to make better, stronger, and more deceptive viruses. The technology behind the virus has come a long way since the 1970's. It's a field yet to be fully explored and appreciated by the computer community. I, for one, hope that people become more aware of the computer virus and that they take measures to protect

"The beauty of the computer virus is that it perfectly mimics a real virus or small organism."

their data. The ideal scenario would be computer companies rewriting their operating systems to be virus-resistant. In the long run, the computer virus may strengthen our defenses against data loss, whether it be due to viruses, trojan horses, power outages, or unauthorized users. My main hope is that the threat of the virus will help curb software piracy and allow software companies to prosper. If a person knows that he stands a chance of being infected by accepting pirated or modem distributed software, he will realize that he's much better off buying the software and receiving the documentation as well.

How The Virus Works

Before I go any further, let me just say that

(continued on next page)

straight from

a virus should be written in assembly language, "C", or any other language that allows low-level functions (byte manipulation, system calls, memory moves). I doubt you can write a virus in BASIC or PASCAL (a trojan horse maybe, but certainly not a virus). Viruses in the future may be written in Prolog or LISP and incorporate artificial intelligence.

As an example, I'll discuss the CyberAIDS virus, which was written purely in 6502 Assembly. CyberAIDS is an "application resident" virus (see **Virus Types**). Most viruses must make themselves permanent in the storage device in order to continue reproduction. See the **Virus Types** section for a detailed description of the various methods that viruses use for reproduction and where they may hide themselves.

After attaching itself to a file or disk that was previously uninfected, the actions of any particular virus may vary, but the virus will check the disk counter before proceeding to any intended action other than reproduction. The disk counter, an individual byte somewhere on the infected disk, keeps track of how many times the virus has accessed that particular disk, and thus assures that the virus will not detonate prematurely. Some viruses are totally harmless and print a simple text message (such as the Macintosh virus), while others are created to cause harm and/or to destroy data (like CyberAIDS). There are still other viruses which were not originally meant to be destructive, but due to the fact that they come between an operating system and its applications, cause harm nonetheless. This harm is usually in the form of system crashes or

the destruction of protected software (i.e., the Amiga virus, which would not affect standard disks but would destroy protected disks due to their non-standard file/disk format).

How The Virus Spreads

All viruses spread. This is what makes them distinct from trojan horses. Whereas a trojan horse program simply wipes out your hard drive when you run it once or twice, a virus will attach itself to normal applications or disks and make them carriers. Care must be taken that the virus will only infect one file each time the infected application runs, thus making sure that the time before the original application executes is kept to a minimum. This will allow the virus to go unnoticed during the user's daily activities. You can run a virus-infected program a hundred times and it will behave normally with the exception that it will make copies of the virus portion and attach itself to other disks/applications, but when you run it the final time, it will perform its intended activity. Since only that copy of the virus has detonated, you are still left with perhaps dozens of infected files which will not detonate until they are run several hundred times (and thus will spread the virus even more).

The benefits of an application resident virus such as CyberAIDS are several. Since no new files are ever created on the disk by the virus, the user will probably not notice anything is wrong. Instead, normal applications are modified by the virus to execute viral code. When individual files (non-text executable code files) are infected, the virus can be spread in three ways:

(1) The manual copying of the file from disk to disk by the user. User-group disk

the source

distribution can achieve the best results when this method of reproduction is used.

(2) The automatic copying of viral code by the virus itself to non-infected files in other drives or the hard disk. Usually serves to give the virus a better foothold within a particular user's software library.

(3) The transfer of infected files over the modem. The infection has a good chance (whether by accident or on purpose) of reaching public domain or pirate bulletin boards. The distribution of that file will be incredible. Infected files may also be spread through LAN's (Local Area Networks).

Application Resident Virus Outline

A. INITIALIZE.

1. Find current location of virus in memory.
2. Relocate itself to predefined memory location.
3. Make sure DOS is active and ready to accept system calls.
4. Move original application header

"The virus may even call its creator and allow the transfer of data from the infected system."

(6 bytes) back to original memory.

B. SEARCH.

1. Choose random volume (disk device).

- a. Make sure volume is not write protected

- b. Make sure volume is on line (no I/O error)

2. Increment disk counter (See NOTE1) and go to destroy (See NOTE2) if necessary.

3. Check for enough space on volume.

4. Choose candidate file.

- a. File must be a system or application file.

- b. File must not be already infected (choose appropriate method for identifying infected files).

- c. File must be small enough to allow viral attachment (so that the application and virus code both fit in memory).

- d. If the file is locked then unlock it.

C. INFECT.

1. Open candidate file.

2. Load first block of candidate file into a main.buffer.

3. Take first (6 bytes) and save to alt.buffer (also known as SH).

4. Calculate viral location in new file.

- a. $Viral.Addr = Application.Start.Addr + Length.of.Application + 6$

5. Store a JUMP Viral.Addr at beginning of file.

6. Rewrite main.buffer.

7. Set file pointer to end of file (for append).

8. Write the alt.buff (6 bytes).

9. Write the viral code afterwards.

10. Close candidate file.

D. DESTROY (Optional).

1. Lock out Keyboard and Reset Key if possible.

(continued on next page)

how to do it

2. Destroy data.
 - a. Recognize all disk devices (hard disks, floppies, 3.5", ram).
 - b. Wipe out the directory (FAT) blocks of each device.
 - c. Wipe out key block for each file in each directory block.
3. Do graphics and music (optional).
 - a. Totally up to virus writer.
4. Present text message (optional).
 - a. Totally up to virus writer.
- E. LEAVE.
 1. Jump back to Application.Start.Addr
 - a. Thus continue as if nothing had happened.

NOTE1: The disk counter is a particular byte on the disk that the virus uses to hold the value of how many times that virus has run with that particular disk inserted (active).

NOTE2: DESTROY or LEAVE is executed depending on the status of the disk counter.

Virus Types

Application Resident:

Hides in applications (see **Virus Outline**). Patches an application (or system file, .EXE, .COM, .SYS file) so that the virus is appended at the end of the file and a call to the virus is provided at the beginning of the file. The original beginning of the file is saved to the end of the file as well, as it will be moved back (SH is moved back to where JC is, see Figure B) into place at the beginning of the file when the virus executes, thus allowing the application to execute normally after the viral chores are completed. Due to the different position of the viral code in each infected file (because of different file lengths) and

unless the viral code can run anywhere in memory, it must be able to relocate itself into a pre-set memory location where it will run.

(a) Normal (not infected file)

```
+-----+-----+-----+
| SH | rest of application | EOF|
+-----+-----+-----+
```

(b) Infected file

```
+-----+-----+-----+-----+
| JC | rest of application | SH | VC |
EOF |
+-----+-----+-----+-----+
```

SH = Standard Header (first few bytes of the original file's executable code).

JC = Jump Code (jumps to the address of the virus).

VC = Viral Code (see **Virus Outline**).

EOF = End of File.

Boot Block Resident:

Activated upon boot. Usually loads additional program code from other blocks on disk. This is quite invisible as files are never altered, and blocks used by the virus on disk are designated as busy for protection. The Amiga virus is a perfect example.

Memory Resident:

Resides in memory. Usually a terminate and stay utility that can be activated by any event (clock, keyboard, DOS call). On multi-tasking systems (such as Unix, Xenix, OS/2) it can be a background task. It will usually allocate memory for itself from the memory manager.

(continued on page 14)

BUILDING A RED BOX

by J.R. "Bob" Dobbs

Essentially, the red box is a device used to fool the phone company into thinking you are depositing coins into a payphone. Every time you drop a coin into a payphone, the phone signals the type of coin inserted with one or more bursts of a combination of 1700 hz and 2200 hz. The tone bursts are coded as follows:

Nickel: One 60 millisecond pulse

Dime: Two 60 millisecond pulses separated by 60 milliseconds

Quarter: Five 35 millisecond pulses separated by 35 milliseconds

How to Use It

Operation is simple. Simply dial a long distance number (some areas require you to stick in a genuine nickel first), wait for the ACTS computer to demand your cash, and press the "deposit" button on the red box for each coin you want to simulate. The coin signals are coupled from the red box into the phone with a small speaker held to the mouthpiece. For local calls, either you must first deposit a genuine nickel before "simulating" more coins or place your call through the operator with 0 + 7d. Use some care when the operator is on the line -- sometimes they catch on to your beeper ploy.

Circuit Operation

Each time the pushbutton is pressed, it triggers half of IC1, configured as a monostable multivibrator to energize the rest of the circuit for a length of time determined by the setting of the coin selector switch. This in turn starts the other half of IC1, configured as an astable multivibrator, pulsing on and off at regular intervals at a rate determined by the 50k pot between pins 12 and 13. The output of the astable thus alternately powers IC2, configured as a square wave oscillator, providing the required 1700 hz and 2200 hz to the op amp which acts as a buffer to drive the speaker.

Construction

Assemble the circuit as you wish. Component placement is not critical. I found the easiest method was to use point-to-point wiring on a "universal" PC grid board with solder ringed holes. Use sockets if you aren't a whiz with a soldering iron. Be sure to leave easy access to the potentiometers for alignment.

Alignment and Testing

For alignment, a frequency counter and triggered sweep oscilloscope are extremely handy (but not *absolutely* necessary).

Install a temporary jumper from +9v supply to pin 14 of IC2 and temporarily disconnect the 0.01uF

(continued on page 22)

how it's done

(continued from page 12)

DOS Resident:

A virus that's patched into DOS and infects any disk, file, or DOS on disk that's accessed during the time that the infected DOS is active. Since DOS is the program which runs on the computer 98% of the time, it would be advantageous to add viral code to a frequently executed portion of DOS (such as Read Block code). The infected DOS will usually attempt to patch any DOS on disk and to make it infected. Care must be taken to prevent crashes, thus making sure the virus will only patch DOS versions that can be successfully altered by the virus. Any unrecognized DOS on a disk should be left alone.

Application Oriented:

A virus that's integrated into an application and works closely with it. Application oriented trojan horses are quite common, but viruses that are integrated into an application are hardly ever seen. For example, a packing (file compression) program such as ARC or a terminal program that infects files before packing or transmitting them.

Types of Viral Action

Complete Disk Data Destruction:

Affects floppy, 3.5", hard disks, ram disks. Usually the most common action taken by a virus. It is quick and is not noticed until it is too late. Care must be taken to prevent the user from prematurely stopping the destruction by locking out the keyboard or by giving a text message that will make them feel comfortable (i.e., "Loading Data Segment", "Checking for files").

Slow Disk Data Degradation:

Similar to above, except data is slowly destroyed on a disk with each activation of the virus. Usually a disk block at a time, but may be done a byte or even a bit at a time. This is perhaps the most sinister viral action as it will take quite a long time before anyone notices anything is wrong. Also known as the "disk bit spray".

Slow Memory Data Degradation:

Data in memory is modified a byte or a bit at a time. Usually done by a memory resident or background task virus. This will slowly destroy program code and data as the person is working at the computer. Weird things may happen and usually data integrity is compromised or program crashes will occur at random times. This is also known as the "memory bit spray".

Hardware Destruction:

A virus will attempt to destroy hardware if possible. It usually attempts things like overloading the address or data bus by attempting to activate all peripheral cards at the same time. "Head Slamming" may also be done, a process which allows older hard disks to have their read/write heads slammed at high velocities into the parking position or into the side of the disk enclosure. If any mechanical parts are present in the computers (relays), the virus will attempt to wear out or jam these devices by turning them on and off at very high speeds. This may also destroy various video and uart chips. Also, the virus will attempt to alter the time and date in any clock card or chip, or even destroy the pre-set configuration in battery-backed ram.

and why

Modem manipulation:

A virus that usually attacks BBS systems and is a memory resident virus. It will activate itself during the time the BBS is not in use and play with the modem and the phone line. It does things like call Europe directly or call the police over and over. This virus may actually cause the infected person to go to jail or increase their phone bill or both. The virus may even call its creator and allow the transfer of data from the infected system.

That concludes this article. I hope you enjoyed it. I would like to see some more viruses out there. To write and distribute a virus you must lose every shred of moral fiber, and if I know the readers of this magazine, there will be a computer virus plague in the very near future. So have fun, kids. If you write a successful virus, don't hesitate to release it, and by all means send the source code to 2600. We'd like to hear from you.

CALL ONE OF OUR COMPUTER BULLETIN BOARDS TODAY!

2600 BBS#1

(OSUNY)

914-725-4060

*

2600 BBS#2

(CENTRAL OFFICE)

914-234-3260

*

2600 BBS#3

(YOYODYNE)

402-564-4518

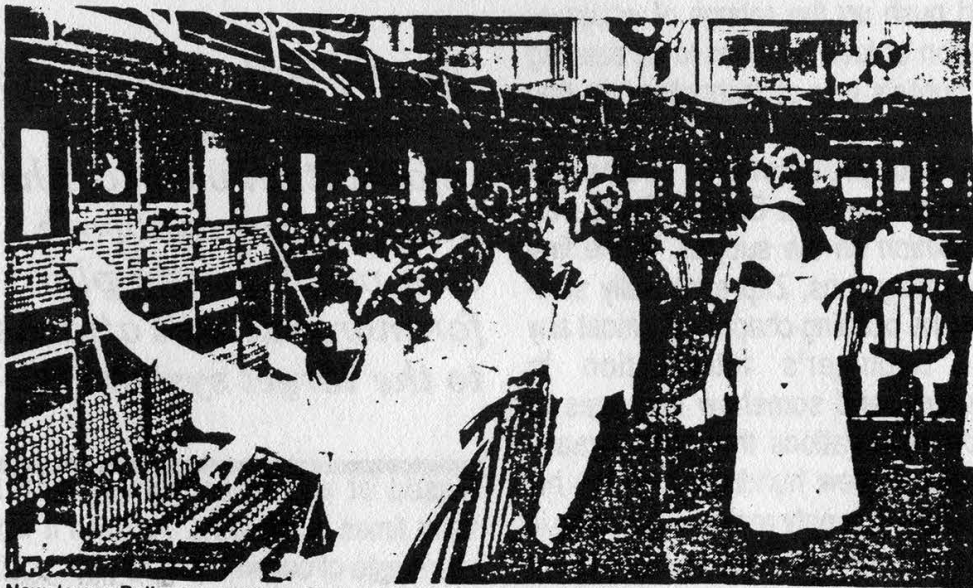
*

2600 BBS#4

(BEEHIVE)

703-823-6591

ALL OPEN 24 HOURS



New Jersey Bell central offices, Church Street, New Brunswick, 1912.

A READER'S REPLY

by The Rancid Grapefruit

Query: "What happens to inept computer criminals who get caught?"

Answer: "They open up 'security' companies and start preaching to an extremely gullible public -- usually casting themselves as some kind of 'hacker expert' whereas the only thing they are 'experts' at is getting caught."

The opening comments have absolutely nothing to do with Captain Zap, whose reputation is impeccable, and we most certainly would not want people to misconstrue the comments as a vicious attack on his person. Lord, no....

Obviously, we disagree with Captain Zap's brilliant observations on the state of "Hacking and Phreaking". If we did agree with him, we'd hardly be writing this swell response, eh?

"The ongoing wave of computer crime that is being reported in the media around the world shows" the shallowness of the media's never ending quest for anything that will titillate a technology-ignorant public, and push up the ratings of whatever publication or feed happens to be catering to the public's fear of technology on that particular occasion.

"An Interpretation of Computer Hacking" is just that: Captain Zap's personal *opinion* on the subject. In the first several paragraphs, Zap essentially summarizes the opening chapter of almost any given "Beginner's Introduction to Computers" and somehow manages to pass off observations that have already been made a few hundred times as his own "ideas". The only real mystery to us is why he decides on "16 Megabytes of RAM" as an arbitrary amount of memory

that "today's personal computers" are supposedly equipped with.

This leads into the "information is power" spiel, and the inevitable arrival of ISDN wherein phones and computers will become one glorious entity and live happily ever after.

All of this ends up with Zap giving you his opinion on "The Dawn of Phreaking", the usual mention of Draper and blue boxing, followed by a summary of the boxes that matches slang to function, and terminating with a simplified account of toll fraud where Zap babbles about the various OCC's for a while.

Although we were very impressed by the programming ingenuity of the supplied "Wargames dialer" listing, and find ourselves constantly looking to the first section of Zap's article when we feel lost or at a need for guidance, we will regrettably have to let it stand. Since aside from the ill-chosen "highlights of yesteryear" there is nothing there that hasn't been dis-

"Rarely is the purpose of a conference to 'pass information over to other hackers that can work on a problem and plan for more tactical attacks to the target system.'"

cussed or otherwise summarized too many times in the past. As such it would be a waste of our time to do so yet again.

Hacker Communications! Shhhhhh!

TO CAPTAIN ZAP

Secrets being exchanged!

While we don't dispute the fact that people do call each other, sometimes in large groups hooked together on a conference (without paying for it, gasp!), *rarely* is the purpose of a conference to "pass information over to other hackers that can work on a problem and compare results and plan for more tactical attacks to the target system." The usual reason a conference starts is because one kid is bored and wants to talk to a bunch of his peers at the same time. What takes places on almost any given conference is a bunch of screaming kids harassing TSPS operators, calling pizza parlors in Europe, and in general pranking or annoying anyone they can think of at the moment.

"Attacks" placed on Bell System computers are usually the result of one kid -- who is *not* some genius, rather he's quite often the friend or relative of somebody who understands the *concepts* involved, not only the commands -- who thinks it would be a blast to turn off CAMA on a few switches, or disrupt COSMOS operations. All of this potential damage is made possible by the RBOC's themselves, which provide extremely minimal security that is more of a study in faulty security techniques and shoddy organization than any kind of obstacle to the potential hacker.

While "computing power" is now within reach of a vast number of people, almost all of that "vast number" are ignorant as to their system's potential. In fact, most never get beyond running their spreadsheet or doing taxes on that wonderful PC with "16 MB RAM". And if they ever do sink into the sordid depths of depravity

and actually try something awful like making a bit copy of someone else's program and xeroxing its manual, it's our personal belief that the world will in all probability not come to an end. Of course, we could be wrong.

Almost all potential hackers are little kids with a lot of time on their hands, and most of those kids will never get anywhere because they are not brilliant, or in any way gifted -- regardless of what the public might think of them. The vast majority of people that the public views as computer geniuses are quite average teenagers whose only "skill" is calling up boards -- with "better security than most large computer systems" -- and blindly applying things they see posted on them, *without* understanding what they are doing. Granted this is a "threat", but it's the *only* threat that boards pose. And the only reason it's a problem to begin with is because the "threatened" organizations or companies have ridiculously bad security.

While it is true that more people now own personal computers than at any other time in history, the overall effect of this influx of new hackers is negligible. Instead of one kid annoying his local CO from information he found on some board, there are 10 kids using the same information from the same board to harass the same CO. In short, there is a deluge of "idiot savants" who are capable of doing no more damage than trained chimps.

The Bulletin Board Systems

Bulletin board systems (BBS's) pose a possible threat for the simple reason that the more highly skilled users will post potentially dangerous information in a

(continued on next page)

A READER'S VIEW

place where the "idiot savants" can read it. The better versed user's reason for posting it is ego gratification. Regardless of what he claims, the only incentive he has to post this information is an ego boost. He already knows that the "idiot savants" are going to do something stupid with the information, at worst simply making it valueless, at best flexing their muscles and showing their target how vulnerable they are to an outside attack.

Granted, if BBS's didn't exist, much of the trouble various people and companies now experience would vanish along with the "idiot savants". But the only thing the boards really do is provide a forum for the more intelligent users to bask in the adoration of fools. They are not some great organized crime wave of the future; they are simply used by several thousand bored kids, the great majority of them trying to live out some kind of power trip while the remaining minority congregate together because they like being surrounded by those they view as their peers.

In summary, boards are a social medium -- not the forefront of some well orchestrated, nationwide attack on loopholes in "the system". Just about any issue of *Soldier of Fortune* contains all the information you could possibly want about where to obtain books on plastic explosives, nerve gas, special weapons, electronic devices, and anything else that has been dreamed up. You hardly need a BBS in order to have access to that kind of knowledge. In fact most of the information posted on the "death and destruction" subs of boards is a word-for-word copy of some article that originally appeared in one of these books. The only crime taking

place is copyright infringement.

Specific Responses to Some of Zap's Statements

Let's cover Zap's statements one by one:

➔ "Such information like dial-up port numbers, logons, and passwords are common information available to the main hacker population." No shit. It's also common information available to anyone who calls up any of the carriers and requests it. The logons and passwords are usually the end result of credit card fraud, and have nothing to do with the ingenuity of hacking into a system.

➔ Zap's entire spiel on board security, the "select few", and the security of hacker boards takes place for the most part in his head and nowhere else. The only reason most people never move into these hallowed ranks is because they have somehow convinced themselves that this isn't possible. The only thing separating you from anything you want to access is ignorance of how the sysops' minds function and the *reality* of how security works, as opposed to the ridiculous fantasies presented by Zap.

Assuming a sysop had no life outside of his board, and he got paid by the hour to sift through all of those records of his potential users, all he'd accomplish would be to weed out people who didn't know how the system worked. Anyone who wanted access and understood the basics of how to falsify information would still gain entry, and the end result is a security breach. *There is no such thing as perfect security.* When *anyone* "builds a better mousetrap", a few days later an inventive person will "build a better mouse".

OF THE ZAP ARTICLE

In any case, the security examples presented by Zap *do not* exist on any private or "elite" phreak or hacker BBS now in existence. If the sysop *claims* that is what they do, it's simply meant to scare potential users into submitting valid information which the sysop doesn't bother to verify beyond the telephone number.

➔ Disclaimers and Clauses: Whether Zap's comments originate from actual ignorance or simply a desire to knowingly misinform, is unknown to us.

A disclaimer, *any* disclaimer, will have very little value in any kind of legal situation. While the sysop might feel better if "it's not my fault" and "for information purposes only!" are splattered over every part of his board, it isn't going to make *any* difference to *any* judge in *any* court! Disclaimers are *not* legally binding. All they do is take up space and lull sysops into a false sense of security.

Thinking you're safe because you have a good disclaimer translates out to "ignorance is bliss". If you haven't had any trouble with law enforcement agencies to date, it only means that they don't know about your existence (buried as you are amongst 1,000 other quasi-legal BBS's), or that they know and don't care because you aren't doing anything that they're worried about.

➔ Tele-Trial: I can't believe this! Zap, where ya been for the last three years? Tele-Trial was a ridiculous "electronic tribunal" started by King Blotto as a joke. For whatever reason, he started taking himself seriously and for a few months in 1985 "Tele-Trials" were being held, in which "electronic execution" took place and stupid kids cried about being thrown

off Blottoland and being declared "un-cool!" (The horror!)

It is *impossible* for anyone to enforce any "ruling" over anyone else in the modem community. The boards are not all interconnected and what one person, or group of people, declares as "law" on one system, or set of systems, is utterly meaningless to the hackers the next area code over. And even to the people involved with those specific systems, it only pertains to them if they want to play the game. There is nothing preventing an "exiled" person from picking up a new handle and starting over.

Aside from the complete impossibility of enforcing such "rulings" over anyone but the most brain-damaged kids, all of this is nothing more than a history lesson.

(continued on next page)

WILL PAY
\$1,000

**FOR EARLIEST INFORMATION
LEADING TO ARREST
AND PROSECUTION
WITHIN NEW YORK AREA OF**

- CALLING ROOM OPERATORS
- BLUE BOX OPERATORS
- COMPUTER HACKING INVADING
LONG DISTANCE TELECOMMUNICATIONS

Call (212) 227-4519
(Between 7:00 A.M. and 11:00 P.M.)
CONFIDENTIALITY STRICTLY MAINTAINED

NEW YORK, NEWSPAPER, MAY 11, 1988
5
Part II/28

**THIS AD APPEARED IN A NEW
YORK NEWSPAPER THIS
SPRING. THE HUNT IS ON!**

RESPONDING TO THE

Tele-Trials have been over since the summer of 1985.

As for Richard Sandza, Tele-Trial still existed at the time of the publishing of his articles for *Newsweek*. The "Tele-Trial" he was put on was simply a conference of abusive kids who felt that he had given hackers unfair treatment. In retaliation they threatened him: a Captain Quieg posted his credit report and numerous kids ran up bills on his credit cards, sending assorted junk to his house.

Hackers cannot "perform the destruction" of *anyone*. All they can do is scare the shit out of "normal" people who are shocked that a bunch of kids can get their unlisted number, credit cards, and various other records, and abuse them.

In any case, Sandza is something of an exception since he managed to piss off a large percentage of people who were in a position to make life hard for him in return. Most people who disagree with him can write a complaint to *Newsweek*, but if you have the ability to bring your displeasure to his personal attention, in a way that will ensure he gives notice to it, wouldn't you do the same thing? After all, it isn't *Newsweek* you're mad at, it's Richard Sandza. Some of you probably wouldn't, but that's one of the fringe benefits of being a hacker. Instead of being bound by "the system's" rules and regulations, you can get around it and let your conscience be your guide (if you happen to have a conscience).

➔ "And remember, the hacker can be the best prevention for computer security sickness and that a reformed hacker can make for the best data processing security person." Another token stab at self-promo-

tion by Zap.

➔ "The boards in general have been a major problem in the control of information due to the use of the boards by what some may call 'information junkies.'" What's wrong with people who want to collect information? Are you suggesting that arbitrary censorship would be an improvement?

➔ "One of the major contributing factors involving computer abuse is the non-education of the users in ethics." While it makes for a nice sweeping generalization, this statement has little to do with reality.

Most "normal users" think no more of copying a piece of software than they think of taping a copy of an album, or xeroxing a page out of a copyrighted publication. While all of these acts are illegal, there aren't many people that actually care. "Educating" people is not going to eradicate these problems.

As far as the phreaks and hackers are concerned, the statement is even more ludicrous. While a minority undoubtedly justify their actions to themselves as "curiosity" and thus set their consciences to rest, the greater percentage know that in the course of doing whatever it is that they happen to be doing at the moment, they are committing crimes. And they don't care.

Morality and ethics are subjects that cannot be "taught" to anyone. Each individual has to make his or her personal choices based upon whatever tenets or beliefs they happen to espouse. Very often people who function from a predominantly logical perspective come to the conclusion that "right and wrong" are relative to a given time and situation. As applied in

CAPTAIN ZAP ARTICLE

our society they typically denote values that most of our present population subscribes to. Why should anyone do something just because everyone else is doing it?

Ethics will always be up to the individual, who will in many cases come to the logical conclusion that he doesn't care what the rest of society condones or accepts, and instead of blindly following their dictums he will choose to think for himself and perhaps arrive at conclusions that don't coincide with what society happens to find acceptable at that particular time.

➔ Accessing government and military computers: Why it is that people come to the conclusion that government computers should be bastions of security we couldn't begin to guess. When you speak of the government and military, we presume you mean *our* government and military; you know, the one run by incompetents, bureaucrats, and other paper pushers that excel at nothing except wasting time and money.

For someone who cautions others against making "rash statements", Captain Zap has apparently written an entire article filled with statements that neatly ignore his own dictum.

Lastly, we'd like to bring up one relevant fact that most "security analysts" manage to ignore: hackers and phreaks (for the most part) are not criminals. At least that isn't the way they view themselves. While nobody lays awake nights worrying about the fact that today he's cost a few phone companies some money, and perhaps wasted system resources on un-authorized applications, a

hacker or phreak's primary motivation is either a real hunger for knowledge, or ego gratification. In neither case does monetary gain enter the picture. The people you really have to worry about are career criminals. They aren't kids and they don't call boards. If a hacker is present in your system, then a criminal could easily gain entry to your system as well. If anything, you should view it as a blessing that the hacker has brought your lack of security to your attention.

The previous paragraph shouldn't be misconstrued as a moral judgment on criminals. Personally we couldn't care less how you make your living as long as you're good at what you do.



Artwork by J.R. "Bob" Dobbs
Red Box article on page 13

HOW TO BUILD

(continued from page 13)

capacitors from pins 5 and 9 of IC2. Power up the circuit. Measuring the output from pin 5 of IC2 with the frequency counter, adjust the 20k pot between pins 1 and 6 for an output of 1700 hz. Now adjust the 20k pot between pins 8 and 13 for an output of 2200 hz from pin 9 of IC2. Remove the temporary jumper and re-attach the capacitors to pins 5 and 9. (Note: if no frequency counter is available, the outputs can be adjusted by ear one at a time by zero-beating the output tone with a computer generated tone of known precision.)

Next, temporarily disconnect the wire between pins 5 and 10 of IC1. Set coin selector switch in the "N" (nickel) position. With the oscilloscope measuring the output from pin 9 of IC1, adjust the 50k pot between pins 12 and 13 of IC1 for output pulses of 60 millisecond duration. Reconnect the wire between pins 5 and 10. (Note: If no scope is available, adjust the pulse rate by ear using computer generated tones for comparison.)

The remaining adjustments are made by ear.

Leave the selector switch in the "N" position. Adjust the 50k pot labelled "Dime" for a quick double beep each time the pushbutton is pressed.

Finally, set the selector to

"Quarter". Adjust the 50k pot labelled "Quarter" until exactly 5 very quick beeps are heard for each button press. Don't worry if the quarter beeps sound shorter and faster than the nickel and dime ones. They should be.

Conclusion

If all went well to this point, your red box should be completely aligned and functional. A final test should now be conducted from a payphone using the DATL (dial access test line) coin test. Dial 09591230 and follow the computer instructions using the red box at the proper prompts. The computer should correctly identify all coins "simulated" and flag any anomalies. With a little discretion, your red box should bring you many years of use. Remember, there's no such thing as space change!

Parts List for Red Box

Semiconductors

- (2) 556 Dual Timer
- (1) 741 Op Amp
- (1) 1N914 Switching Diode

Resistors

- (6) 10k (1) 4.7k
- (2) 100k
- (4) 50k PC Mount Potentiometer
- (2) 50k Multi-Turn Potentiometer

Capacitors

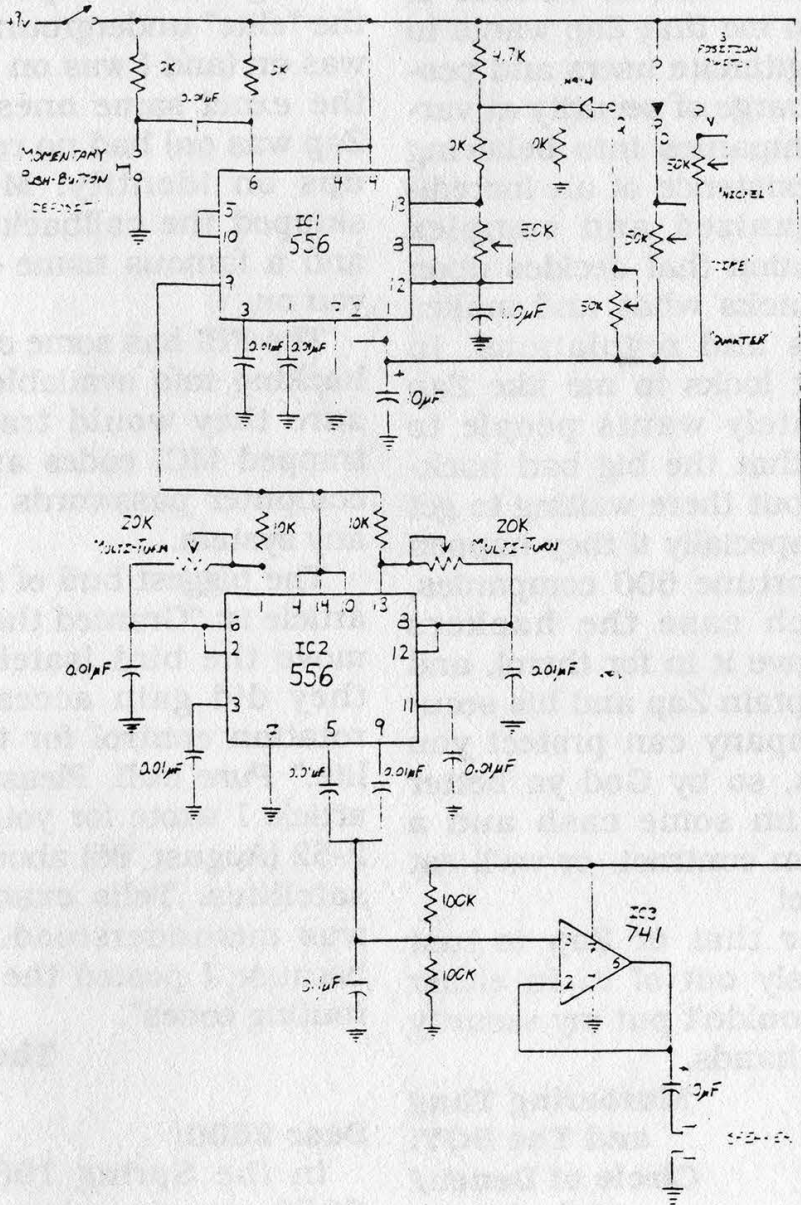
- (10) 0.01 uF (1) 1.0 uF
- (2) 10.0 uF Electrolytic

Miscellaneous

- (2) 14 Pin Dip Socket

A RED BOX

- | | |
|--|-----------------------------------|
| (1) 8 Pin Dip Socket | (1) Speaker or Telephone Earpiece |
| (1) 3-position Rotary Switch | Circuit Board |
| (1) Momentary Push-Button Switch (normally open) | Box |
| (1) SPST Toggle Switch | Mounting Hardware |
| | 9V Battery Clip |



THESE ARE

Reactions to Zap

Dear 2600:

After reading Captain Zap's article in your last issue I'm left with the feeling that it was not meant to inform. Rather it seems to me that Zap wants to scare legitimate users and people in charge of security at various companies into believing in the existence of an incredibly organized and complex organization that decides upon who attacks what and makes up laws and regulations. In short, it looks to me like Zap desperately wants people to believe that the big bad hackers are out there waiting to get them (especially if they happen to be Fortune 500 companies, in which case the hackers *really* have it in for them), and only Captain Zap and his security company can protect you from us, so by God ya better hand him some cash and a long term contract, or we'll eat you alive!

Either that or Zap is just hopelessly out of it. In either case I wouldn't put my security into his hands.

**Murdering Thug
and The BOY!
Circle of Deneb/
Digital Gang**

Dear 2600:

Is Captain Zap for real? Is this the same Captain Zap who used to go by the name of Ian Murphy and is consulting on computer security? It's a pretty far-fetched picture of an evil underground conspiracy. All of the "elite" underground BBS's I was on (and I was on several of the *exact* same ones Captain Zap was on) had no real check-ups on identity. Most even skipped the callback to verify and a famous name could get you on.

The FBI has some of the best hacking info available and I'm sure they would trade a few trapped MCI codes and traced computer passwords to get on any system.

The biggest bull of the whole article is: "Granted they did not move the bird [satellite], but they did gain access to the rotation control for the satellite." *Pure* bull. Please see the article I wrote for you on page 2-52 (August '85) about moving satellites. Tells exactly what was misunderstood. I know, because I posted the "satellite routing codes".

The Shadow

Dear 2600:

In the Spring 1988 issue, 2600 presented an article called "The Hacker Threat"

THE LETTERS

written by Captain Zap. While I don't agree with the article, I'm glad you published it because I like to see different opinions which provoke discussion. After reading the article I decided to do a little research on him.

Captain Zap, whose true name is Ian Murphy, is now a computer security consultant. This was not always true. Until the time of his arrest, he was a hack (Taxi Driver) by trade and a hacker by hobby. In 1984 he was convicted of credit card fraud. Now, as a reformed hacker, he *attempts* to help companies free their systems from hackers. Recently, he has been active on many BBS's, including those sponsored by 2600. On Central Office BBS he claimed that a rival computer security consultant from Detroit had been charged with criminal sexual conduct and harassment. He then threatened to sue that same consultant for alleged slander. He also vigorously attacked The Telecom Security Group (TTSG), a respected Newburgh (NY) based consulting firm, for having advertised in 2600 and for being closely involved with computer hackers. TTSG is considering legal action against Murphy.

Murphy has been profiled by

such periodicals as *The Wall Street Journal* and *USA Today*. In these interviews he has admitted to such acts as: monitoring his ex-wife's telephone with an illegal wiretap, breaking and entering a client corporation's facilities, and refusing to turn in information about alleged criminals.

I hope this is of interest.

Yevgeny Zamyatin

For a reply to last issue's Captain Zap article, turn to page 16.

Gripes and Feedback

Dear 2600:

Hi. I am one of your numerous subscribers and interested readers who has a few gripes with the Spring 1988 issue of 2600.

Although I don't mind the new format and appreciate its larger size I think it could stand somewhat better editing.

"The Threat of Computer Hackers." One or two nice anecdotes but the rest should have gone into *Byte* or *Compute!* I mean you can assume that you have more enlightened readers on that subject that don't need a "HCK-100 BBS & Systems Intro".

(continued on next page)

YOUR

"ROLM Phone System." You could have cut this to one or two pages. About 50 percent of the article is fluff, like the complaints that people can't use the new phone with those weird buttons. Times change faster than humans and some of the complaints are hardly worthy of the reader's time. So what if the info number changes from 246-3636 to 632-6830?

Given a larger magazine this wouldn't be so bad, but 2600 is relatively small and so I'd prefer more and shorter articles (if they exist).

OK. What I LIKED: "Monitoring TVRO." Although I am no phreak I love to read stuff like that just to keep informed.

"VM/CMS." Although I hope I will never be on a system like that it might come in handy sometime.

"Weathertrak." Not my real interest, but interesting nevertheless.

"From the 2600 Files." Fun and informative.

"Happenings" and "Letters". These are my favorites.

I hope you don't mind a little feedback from a reader.

Best of luck to you and your mag.

Natuerlich!

We never mind getting comments and criticism. It shows that our subscribers are reading the magazine. What more could we ask for?

We presented Captain Zap's article ("Threat of Computer Hackers") not as a revelation but as an example of what is being said by some. We did this with the intention of opening up a dialogue which, judging from the response in this issue and on the boards, is precisely what happened.

The ROLM article was meant to illustrate more than the simple inconvenience of having to adjust to something new. We were attempting to point out how it's becoming increasingly common for the installers of such systems to blatantly disregard the needs of the users and just assume everyone will figure it out in the end. Being denied the freedom to select an easy-to-remember phone number seemed particularly ironic, considering user flexibility was one of the "advantages" of this new phone system.

By the way, another page that we got lots of comment on was the reprint of our six-cent RCI phone bill that's been showing up faithfully here every month for nearly two years. Well, guess what? RCI must be reading these pages

LETTERS

because we suddenly stopped getting them. (Maybe we should reprint our \$200 MCI bill and hope that goes away!)

A Useful Trick

Dear 2600:

Just a note from a subscriber. I love 2600. It gives a lot of food for thought.

A contribution: On the AT&T Horizon PBX (lately discontinued) there is a "toll-restriction" feature. Ports can be connected to a special card that enforces toll-restriction: i.e., you can't dial 1+ for long distance. The software knows about this too. If you try to dial 1+, you'll get a fast busy tone to let you know it's forbidden. However, the hardware is expensive to modify and it's the software that gives the busy tone, so many companies just let the software do the toll-restriction and don't bother buying the special hardware.

Mistake. If you are on such a system and get the fast busy, just hang on the line for about 30-45 seconds. Presto! Unrestricted dial tone. Most people give up when they hear the fast busy.

Also, here in Atlanta the digital exchanges (Northern Telecom DMS-100's) are programmed so that 940-xxxxxxx

(where x is any digit) will tell you the number you're calling from.

Have fun and keep up the good work.

Your little trick for getting an unrestricted dial tone is probably the single most common technique that exists. And what's so remarkable about it is that so many companies seem completely unable or even unwilling to put a stop to it! We urge our readers to try this on any system that offers any kind of dialing restrictions. Please let us know what you find.

We appreciate the ANI (Automatic Number Identification) information. If readers from other parts of the country know what their ANI numbers are, please let us know. (In the New York metro area, it's 958.)

"Deluxe" Call Waiting

Dear 2600:

Enclosed is another example of how Ma Bell loves screwing the telecommunicating public. This was clipped from "On Line Today", the Compuserve magazine. On one page is a letter in which the writer thanks another correspondent for advice on temporarily suspending call

(continued on page 39)

Protection From

(continued from page 7)

I guess the programmer involved was too cowardly to take me up on my offer and prefers to hurt people not capable of fighting back. I should have known that, I suppose, but I don't normally think of people who attack innocents. Normally, I think of people to respect, not people to pity, certainly not people who must cause such damage in order to "get off".

They are below contempt, obviously, and can do little to help themselves out of the mire they live in.

Still, a worm is a worm.

About FLUSHOT A Brief History

The original incarnation of FLUSHOT was a quick hack done in my spare time. It had a couple of bugs in it which caused it to trigger when it shouldn't, and a few conditions which I had to fix. A strangeness in how COMMAND.COM processed certain conditions when I "failed" an operation caused people to lose more data than they had intended -- certainly not my intent!

"No matter what software protection you use, somebody will find a way around it one day."

FLUSHOT was modified and became FLUSHOT2. It included some additional protections, protecting some other important system files, and protecting against direct disk writes which can be used to circumvent FLUSHOT's protection mecha-

nisms.

Additionally, FLUSHOT2 forced an exit of the program currently running instead of a fail condition when you indicated that an operation should not be carried out.

FLUSHOT2 was also now distributed in the popular archive format (have you remembered to send your shareware check in to Phil Katz for his efforts? You really should. It ain't that much money!).

Next came FLUSHOT3. A bug was fixed which could have caused certain weird things when you denied direct disk I/O to certain portions of DOS 3.x.

The enhancements to FLUSHOT3 included the ability to enter a 'G' when FLUSHOT was triggered. This allowed FLUSHOT to become inactive until an exit was called by the foreground task. So, when you used some trustworthy program which did direct disk I/O, you wouldn't be pestered with constant triggering after you enter the 'G'. Primarily this was a quick hack to allow programs such as the FORMAT program to run without FLUSHOT being triggered each time it tried to do any work it was supposed to.

Additionally, a CMOS RAM check was installed. If a foreground program attempted to change CMOS memory, you'd be advised.

What the heck is CMOS memory, you might be asking. Good question. In AT class and better machines, certain important parameters (such as the type of hard disk you're using, or how much memory there is in your machine) are stored up in special non-volatile memory, called CMOS.

If this gets changed, you might have a problem when you reboot. FLUSHOT3

Computer Viruses

sends at least one little slimebucket back to the drawing board, because it will restore the CMOS and prevent this hassle from occurring.

FLUSHOT+ Features and Enhancements

This release of FLUSHOT has a new name: FLUSHOT+. Because FLUSHOT4 was a Trojan, I opted to change the name. Besides, FLUSHOT+ is the result of some real effort on my part, instead of being a part-time quick hack. I hope the effort shows.

FLUSHOT is now table driven. That table is in a file which I call FLUSHOT.DAT. It exists in the root directory on your C: drive. However, I'll advise you later on how to change its location so that a worm can't create a Trojan to modify that file.

This file now allows you to write and/or read protect entire classes of programs. This means that you can write protect from damage all of your *.COM, *.EXE, *.BAT, and *.SYS files. You can read protect all of your *.BAT files so that a nasty program cannot even determine what name you used for FLUSHOT+ when you invoked it!

Additionally, you can now automatically check programs when you first invoke FLUSHOT+ to determine if they've changed since you last looked at them. Called checksumming, it allows you to know immediately if one of the protected programs has been changed when you're not looking. Additionally, this checksumming can even take place each time you load the program for execution.

Also, FLUSHOT+ will advise you when any program "goes TSR". TSR stands for "Terminate and Stay Resident", allowing

pop-ups and other useful programs to be created. A worm could create a program which leaves a bit of slime behind. Programs like Borland's SideKick program, a wonderful program and certainly not a Trojan or virus, is probably the best known TSR. FLUSHOT+ will advise you if any program attempts to go TSR which you haven't already registered in your FLUSHOT.DAT file.

Finally, FLUSHOT+ will also now pop-up a little window in the middle of your screen when it gets triggered. It also will more fully explain why it was triggered. The pop-up window means that your screen won't get screwed up beyond recognition -- unless you're in graphics mode when it pops up. Sorry, 'dems the breaks!

Registering FLUSHOT+

FLUSHOT+ is not a free program. You're encouraged to use it, to distribute it to your friends and co-workers. If you end up not using it for some reason, let me know why and I'll see if I can do something about it in the next release.

But, the right to use FLUSHOT+ is contingent upon you paying for the right to use it. I ask for ten dollars as a registration fee. This entitles you to get the next update shipped when available. And allows you to pay me, in part, for my labor in creating the entire FLUSHOT series. I don't expect to get my normal consulting rate or to get a return equal to that of other programs which I've developed and sell through more traditional channels. That's not my intent, or I would have made FLUSHOT+ a commercial program and you'd be paying lots more money for it.

Some people are uncomfortable with

(continued on next page)

A Flu Shot For

the shareware concept, or believe that there ain't no such thing as Trojan or virus programs, and that a person who profits from the distribution of a program such as FLUSHOT must be in it for the money.

I've created an alternative for these folks. I'll call it "charityware" [first called that, to my knowledge, by Roedy Green]. You can also register FLUSHOT+ by sending me a check for \$10 made out to your favorite charity. Be sure to include a stamped and addressed envelope. I'll forward the monies onto them and register you fully.

Of course, if you wish, you can send me a check for more than \$10. I'll cash it gladly (I'm no fool!).

Site Licensing of FLUSHOT+

So, you run the computer department of a big corporation, you got a copy of FLUSHOT+, decided it was wonderful and that it did everything you wanted and sent in your ten bucks. Then you distributed it to your 1000 users.

Not what is intended by the shareware scheme. *Each* site using FLUSHOT+ should be registered. That's ten bucks a site, me bucko! Again, make the check out to charity if you're uncomfortable with the idea of a programmer actually deriving an income from their work.

However, if you've really got 1000 computers, you should give me a call. As much as I'd like to get \$10 for each site, that wouldn't be fair to you. So, quantity discounts are available.

The FLUSHOT.DAT file

FLUSHOT+ is table-driven by the contents of the FLUSHOT.DAT file. This file normally exists in the root directory of your C: drive (C:\FLUSHOT.DAT).

A little later in this article you'll see how to disguise the data file name, making life tougher for the worms out there. But for the purpose of this article, we'll assume that the file is called C:\FLUSHOT.DAT.

The FLUSHOT+ program will read this data file exactly once. It reads the data from the data file into memory and overwrites the name of the data file in so doing. A little extra protection in hiding the name of the file.

This data file contains a number of lines of text. Each line of text is of the form:

(Command)=(filename)(options)

Command can be any one of the following characters:

P - Write Protect the file named.

R - Read Protect the file named.

E - Exclude the file named from matching P or R lines.

T - The named file is a legitimate TSR.

C - Perform checksum operations on the file named.

The filename can be an ambiguous file if you wish for all commands except the 'T' and 'C' commands. This means that:

C:\level1*.COM

will specify all COM files on your C: drive in the level1 directory (or its sub-directories). Specifying:

C:\level1**.EXE

would specify all EXE files in subdirectories under the C:\level1 directory, but would not include that directory itself.

You can also use the '?' operator to specify ambiguous characters as in:

?:usr\bin\?.COM

which would be used to specify files on any drive in the \usr\bin directory on that drive. The files would have to be single let-

Personal Computers

ter filenames with the extension of 'COM'.

Ambiguous file names are not allowed for the 'T' and 'C' options.

Protecting files from Write Access

Use the 'P=' option to protect files from write access. To disallow writes to any of your COM, EXE, SYS, and BAT files, specify lines of the form:

P=*.COM

P=*.EXE

P=*.SYS

P=*.BAT

which protects these files on any disk, in any directory.

Protecting files from Read Access

Similarly, you can use the 'R' command to protect files from being read by a program (including the ability to 'TYPE' a file!). To prevent read access to all of your BAT files, use a line such as:

R=*.BAT

Combinations of R and P lines are

"I challenge them to upload a virus or other Trojan horse to my BBS that I can't disarm."

allowed, so the combination of the above lines would prevent read or write access to all batch files.

Excluding files

Programmers in particular should find usage for the 'E' command. This allows you to exclude matching filenames from other match operations. Assume you're doing development work in the C:\develop directory.

You could exclude FLUSHOT+ from being triggered by including a line such as:

E=C:\develop*.*

Of course, you might have development work on many disks under a directory of that name. If you do, you might include a line which looks like:

E=?:\develop*.*

or

E=*develop*

Checksumming files

This line is a little more complicated than others and involves some setup work. It's worth it, though!

A checksum is a method used to reduce a file's validity into a single number. Adding up the values of the bytes which make up the file would be a simple checksum method. Doing more complex mathematics allows for more and more checking information to be included in a test.

If you use a line on the form:

C=C:\COMMAND.COM[12345]

then when FLUSHOT+ first loads it will check the validity of the file against the number in the square brackets. If the checksum calculated does not match the number presented, you'll be advised with a triggering of FLUSHOT, which presents the correct checksum.

When you first set up your FLUSHOT.DAT file, use a dummy number such as '12345' for each of the files you wish to checksum. Then, when you run FLUSHOT, you should copy down the "erroneous" checksum presented. Then, edit the FLUSHOT.DAT file and replace the dummy number with the actual checksum value you had copied down. Voila! If even one byte in the file is changed, you'll

(continued on next page)

Controlling the

be advised the next time you run FLUSHOT+.

But wait! There's more!

When a "checksummed" file is loaded by MS-DOS, it will, by default, be checksummed again. So, if you had a line such as:

```
C=C:\usr\bin\WS.COM[12345]
```

the venerable old WordStar program (still my editor of choice!) would be checksummed each time you went to edit a file.

Of course, you might not want the overhead of that checksumming to take place each time you load a program. Therefore, a few switches have been added. The switches are placed immediately after the ']' in the checksum line:

```
C=C:\usr\bin\WS.COM[12345](switch)
```

These switches are:

,n: will only checksum the file only 'n' times. Only one digit allowed.

-: only checksum this file when FLUSHOT+ first loads. ',1' and '-' are equivalent.

+: only checksum this file when it is loaded and executed, not when FLUSHOT+ first loads.

Therefore, if you wished to only check your WS.COM file when you first loaded the FLUSHOT+ program, you'd specify a line as:

```
C=C:\usr\bin\ws.com[12345],1
```

or

```
C=C:\usr\bin\ws.com[12345]-
```

If you wished to checksum your program called "MYPROG.EXE" only when it was used, try:

```
C=C:\path\MYPROG.EXE+
```

Registering a TSR program

Any unregistered TSR program which is run after FLUSHOT+ will cause a trigger when they "go TSR". You can register a program so no trigger goes off by specifying it in a line such as:

```
T=C:\usr\bin\tsr\sk.com
```

which will keep FLUSHOT+ from complaining about sk.com. Make sure to take a look at the '-T' option, specified in the next section.

Protecting the FLUSHOT.DAT file

Obviously, the weak link in the chain of the protection which FLUSHOT+ offers you is the FLUSHOT.DAT file.

You would think that you'd want to protect the FLUSHOT.DAT file from reads and writes as specified above. However this, too, leaves a gapping security hole: memory could be searched for it, and it could be located that way. A better alternative exists. In the distribution package for FLUSHOT+ exists a program called FLUPOKE.COM. This program allows you

HOLLAND BBS'S by John Drake

Miscclub Benelux BBS	80 64 73 63 (3/12)
Amsterdam	20 15 41 54
Rozenburg	18 19 18 16 8
Amersfoort	33 75 54 44
Eindhoven	40 48 17 92
Leiden	71 12 51 25
Sittard	47 55 20 41
Arnhem	85 23 33 77
Kampen	52 02 24 38 0
Groningen	50 14 51 45
Hoom	22 90 34 04 6
Almelo	54 90 62 54 2
Middelburg	11 80 34 33 6
Venlo	77 82 25 22
Zoetermeer	79 51 04 25 (3/12)
Apeldoorn	55 21 18 11
Den Haag	70 29 50 88
Herpen	41 23 23 32
Alkmaar	72 12 67 83
Rotterdam	10 48 34 25 6
Gouda	18 20 22 31 4
Emmen	59 10 21 00 0
CP/M gg	74 42 38 60 (3)
IBM PC gg	22 86 14 21 (3)
MSX gg	20 98 25 02 (3)
Sharp/MZ gg	32 40 38 86 6
CP/M-SWBoss 70 69 40 81	
P2000 gg	10 47 05 73 2
Olivetti gg	79 51 75 75
Apple gg	15 62 24 21 (3)
NOS Hobby Scoop	35 45 39 5 (3)
Fido Gerard	47 84 23 01 (3)
Fido John	40 53 14 53 (3)
Fido Santech	34 89 83 9

Epidemic

to specify the new name you wish to call the FLUSHOT.DAT file. Simply type:

FLUPOKE (flushot name)

where (flushot name) represents the full path filename of your copy of FLUSHOT+.

You'll be prompted for the name of the FLUSHOT.DAT file. Enter the name you've selected (remember to specify the disk and directory as part of the name). Voila! Nothing could be easier.

Protection Recommendations

Here's a sample FLUSHOT.DAT file, basically the same one included in the archive. Your actual checksums will differ, and you may want to modify what files and directories are protected. Obviously, your exact needs are different than mine, so consider this a generic FLUSHOT.DAT:

```
P=*.bat
P=*.sys
P=*.exe
P=*.com
R=*AUTOEXEC.BAT
R=*CONFIG.SYS
E=?\dev\*
C=C:\COMMAND.COM[12345]-
C=C:\IBMBIO.COM[12345]-
C=C:\IBMDOS.COM[12345]-
```

Running FLUSHOT+

For extra protection, after you've run FLUPOKE, you should rename the FLUSHOT+ program to something unique and meaningful to you, but not a worm.

Assuming you didn't rename it, however, you could invoke the program simply by typing:

FSP

when at the prompt. That's all there is to it. When you're satisfied, you can add it to your AUTOEXEC.BAT file, after all of

your trusted programs have run.

But there are some options you should know about:

Checking CMOS - How often?

The CMOS, as described earlier in this article, is a spot wherein a worm can just make things a bit miserable for you when you next boot your system. However, FLUSHOT+ allows you to protect the contents of your CMOS against such a worm.

CMOS only exists on AT class and better machines!!!

You must specify the '-C' option when you invoke the FLUSHOT+ program in order to have your CMOS safeguarded. There is a check done whenever DOS is accessed to determine if the CMOS has changed. This causes a slight performance penalty. However, this only happens once every 128 DOS accesses. You can modify this ratio, to more or less, by specifying a number after the '-C':

FSP -C10

will check CMOS every ten accesses.

Intercepting Direct Disk Writes Through INT13

The default operation of FLUSHOT+ is to intercept and examine every call to the direct disk routines. You can disable this by including the '-F' switch on your command line:

FSP -F

This is not recommended, but exists primarily for developers who can't use the constant triggering one of their programs may cause.

What about INT26?

Similarly, the same exists for the direct writes which normally are only made by DOS through interrupt 26. Again, I do not recommend you disable the checking, but

(continued on next page)

Virus and Trojan

if you desire to do so, use the '-D' switch.

Turning off the header message

If you've no desire to see the rather lengthy welcome message which is displayed when you first use FLUSHOT+, use the '-h' switch.

Allowing Trusted TSR's to Work

Normally, you'd load all of your trusted TSR's before FLUSHOT+ is loaded from within your AUTOEXEC.BAT file. However, you might want to use SideKick once in a while, removing it from memory as you desire. This could cause some problems, since SideKick, and programs like it, take over certain interrupts, and FLUSHOT+ could get confused about whether this is a valid call or a call that shouldn't be allowed. Normally, FLUSHOT+ will trigger on these calls, which is safer, but can be annoying. If you use the special '-T' switch upon program invocation, then calls which trusted TSR's (those specified with the 'T=' command in your FLUSHOT.DAT file) make will be allowed. Understand, please, that this basically means that calls made by a Trojan while a trusted TSR is loaded may not be caught. Please, use this switch with caution!

Disabling FLUSHOT+

There may be times when you're about to do some work which you know will trigger FLUSHOT+. And you might not want to be bothered with all of the triggering, the pop-up windows, and your need to respond to each trigger. If you look in the upper right hand corner of your screen, you'll see a '+' sign. This indicates that FLUSHOT+ is monitoring and attempting to protect your system. Depress the ALT key three times. Notice that the '+' sign

turned into a '-'? Well, FLUSHOT+ is now disabled, and will not trigger on any event. If you depress the ALT key three more times, you'll see the '-' turn back into a '+' - each time you depress the ALT key three times, FLUSHOT+ will toggle between being enabled and disabled.

Disabling FLUSHOT+ Toggle Display

Alas, there are graphics applications

"All of the protection I had would have been for naught if I didn't use the first line of defense from these worms: full and adequate backup."

which will be screwed up by the '-' or '+' in the upper right hand corner of your display. Therefore, if you depress the CTRL key three times, you'll be able to toggle the display capability of FLUSHOT+. The default configuration of FLUSHOT+ is to "come up" with display turned on. You can reverse this capability if you include the '-G' (for graphics) switch on your command line when you run FLUSHOT+.

Interpreting a FLUSHOT+ Trigger

So, you've run FLUSHOT+, and you're at your C> prompt. Great! Now stick a blank disk which you don't care about into your A: drive and try to format it.

Surprise! FLUSHOT+ caught the attempt! You have three choices now: typing 'Y' allows the operation to continue, but the next one will be caught as well.

Prevention 1003

Typing a 'G' (for Go!) allows the operation to continue, disabling FLUSHOT+ until an exit from the program is made. When FLUSHOT+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

Any other key will cause a failure of the operation to occur.

When you've got FLUSHOT+ running and you get signaled that there is a problem, you should think about what might have caused the problem. Some programs, like FORMAT, or the Norton Utilities, PC-Tools, or DREP have very good reasons for doing direct reads and writes to your hard disk. However, a public domain checkbook accounting program doesn't. You'll have to be the judge of what are legitimate operations and which are questionable.

There is no reason to write to IBMBIO or IBMDOS, right?

Wrong!

When you format a disk with the '/S' option, those files are created on the target diskette. The act of creating, opening up, and writing those files will trigger FLUSHOT+ as part of its expected operation. There are many other legitimate operations which may cause FLUSHOT+ to trigger.

So will copying a COM or EXE file if you have those protected with a 'P=' command. FLUSHOT+ is not particularly intelligent about what is allowed and what isn't. That's where you, the pilot, get to decide.

Here's a fuller listing of the messages which you might see when you're using FLUSHOT+:

Checking ===)(filename)

This message is displayed as

FLUSHOT+ checks the checksum on all of the "C=" files when you first invoke FLUSHOT+. The files must be read in from disk, their checksum calculated and then compared against the value you claim the checksum should equal.

If the checksum does *not* equal what you claim it should (which means that the file may have been written to and might therefore be suspect), a window will pop up in the middle of your screen:

Bad Checksum on (filename)

Actual Checksum is: (checksum)

Press "Y" to allow, "G" to go till exit, any other key to exit.

This message simultaneously advises you there is a problem with the checksums not matching, shows you what the checksum should be, and then awaits your response.

Except for the initial run of FLUSHOT+, if you type a 'Y' or a 'G', then the program will load and execute. Typing any other key will cause the program to abort and you will be returned to the C> prompt. When FLUSHOT+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

If this is the initial run of FLUSHOT+, however, you'll be advised of the program's actual checksum, but FLUSHOT+ will continue to run, checking all remaining "C=" files in the FLUSHOT.DAT file.

If you're running a program and you see a screen like:

? WARNING! TSR Request from an unregistered program!

Number of paragraphs of memory requested (in decimal) are: (cnt)

(Press any key to continue)

you're being advised that a program is

(continued on next page)

Controlling the

about to go TSR. If this is a program you trust (such as SideKick, or KBHIT, or a host of other TSR programs you've grown to know and love), then you should consider installing a "T=" line in the FLUSHOT.DAT file so that future runs of this program will not trigger FLUSHOT+.

However, if you get this message when running a program you don't think has any need to go TSR (such as the proverbial checkbook balancing program), you should be a little suspicious. Having a TSR program is not, in and of itself, something to be suspicious of. But having one you don't expect --- well, that's a different story.

Most TSR's "hook into" an interrupt vector before they go TSR. These hooks might intercept and process key strokes ("hotkeys"), or they might hook and intercept direct disk writes themselves. In any event, FLUSHOT+ (in this version!) doesn't have the smarts to do more than advise you of the TSR'ing of the program. If you're truly suspicious, reboot your machine immediately!

If a program attempts to write directly to the interrupts which are reserved for disk writes, FLUSHOT+ will also be triggered and you'll see something like:

Direct Disk Write attempt by program other than DOS!

(From Interrupt (xx))

Press "Y" to allow, "G" to go till exit, any other key to fail.

where the (xx) represents either a 13 (indicating a direct BIOS write to the disk) or a 26 (indicating a direct DOS write). Again, pressing a 'Y' or a 'G' allows the operation to continue, pressing any other key will cause the operation to return a

failed status to DOS, and the operation will not take place. When FLUSHOT+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

If an attempt is made to format your disk, which may be a legitimate operation made by the DOS FORMAT program, you'll see a message such as:

Disk being formatted! Are You Sure?

Press "Y" to allow, "G" to go till exit, any other key to fail.

which follows similarly to the direct disk write operations. You should question whether the format operation is appropriate at the time and take whatever action you think is best.

If one of your protected files is about to be written to, you'll see a message like:

**Write access being attempted on:
(filename)**

Press "Y" to allow, "G" to go till exit, any other key to fail.

where (filename) represents the file you're trying to protect from these write operations. Your red flag should fly, and you should question why the program currently running should cause such an operation.

You may also see the same type of message when one of your "Read-Protected" files is being accessed:

**Read Access being attempted on:
(filename)**

Press "Y" to allow, "G" to go till exit, any other key to fail.

Again, the same red flag should fly, but it doesn't mean that you're infected with some nasty virus program! It could be something harmless or intended. You'll have to be the judge.

Infection

Finally, you may see a message like:

CMOS has been changed!

Hit "Y" to continue, any other key to restore CMOS.

which indicates that your CMOS has been changed while you weren't looking. Or maybe you were: if you're running a setup program which changes the date or the time, or the disk type attached to your AT class machine, this message should pop up. Losing your CMOS is not fatal, but can be an annoyance. If you hit a 'Y', then the new setting of the CMOS will be stored and you'll be able to continue, with alerts to any other change to the CMOS. Any other key will result in the original setting of the CMOS being restored.

How Good is FLUSHOT+, Really?

FLUSHOT+ is a pretty handy piece of code. But it can't absolutely protect you from a worm. No software can do that.

There are ways around FLUSHOT+. I'm of two minds about discussing them, since the worms out there are reading this, too. So I'll only discuss them in passing. And I'll tell you what I use here to protect myself from worms. First, though, a little story to tell you what it's like here, and

how I protect myself from getting wormed.

The RamNet Bulletin Board System site I run is open access. No need to register, or to leave your phone number or address, although a note to that effect is always appreciated. As mentioned above, I dare the worm to try to affect the disk of somebody who can fight back. A couple of worms have tried and I have a nice collection of Trojans and viruses. Obviously, I run FLUSHOT+ on my board, along with checking incoming files with CHK4BOMB. My procedure for testing out newly uploaded code involves me doing a backup, installing all sorts of software to monitor what is going on, and doing a checksum on all files on the disk. I then try out all of the code I get, primarily to determine if the code is of high enough quality to be posted. After testing out all of the week's uploads, I run the checksum program again to determine if any of my files might have been modified by a worm's virus program.

Recently, what looked like a decent little directory lister was posted to the board. For some reason I've yet to fathom, directory aid programs seem to be the ones

(continued on next page)

To obtain more information on FLUSHOT+, contact Ross Greenberg at Software Concepts Design, 594 Third Avenue, New York, NY 10016.

Or call his BBS at (212) 889-6438

1200/2400 N/8/1

Your Computer Could Be Next

which have the highest percentage of Trojans attached to them.

This directory aid program listed my directories in a wonderful tree structure, using different colors for different types of files. Nice program. When it exited, however, it went out and looked for a directory with the word "FLU" in it. Once it found a directory with a match in it, it proceeded to try to erase all of the files in that directory. An assault! No big deal. That's what backups are for.

But it brings up an interesting point: I was attacked by a clever worm, and it erased a bunch of files which were pretty valuable. All of the protection I had would have been for naught if I didn't use the first line of defense from these worms: full and adequate backup.

I've spent three years of my life developing one particular software package. Imagine what would have happened if that had been erased by a worm! Fortunately, I make backups at least once a day, and usually more frequently than that. You should, too.

Now, I quarantine that machine as well. I spent a couple of dollars and bought a bunch of bright red floppy disks. The basic rule around here is that Red Disks are the only disks that go into the BBS machine, and the Red Disks go into no other machine. You see, I *know* that there is some worm out there who is gonna find some way to infect my system. No matter what software protection I use, there *is* a way around it.

You needn't be concerned though -- you're making backups on a regular basis, right? And you aren't asking for trouble. I am, I expect to find it, and it is sort of

amusing to see what the worms out there are wasting their efforts on.

At this point, Trojans and viruses are becoming a hobby with me: watching what the worms try to do, figuring out a way to defend against it, and then updating the FLUSHOT series.

However, there is a possibility that the FLUSHOT series (as well as other protection programs which are just as valuable) are causing an escalation of the terms of this war. The worms out there are sick individuals. They must enjoy causing the damage they do. But they haven't the guts to stand up and actually do something in person. They prefer to hide behind a mist of anonymity.

But you have the ultimate defense! No, not the FLUSHOT+ program.

Full and adequate backups!

There are a variety of very good backup programs which can save you more work than you can imagine. I use the FASTBACK+ program, which is a great little program. I backup 30 megs once in a while, and do an incremental backup on a very frequent basis. There are a variety of very good commercial, public domain, and shareware backup programs out there. Use them! Because, no matter what software protection you use, somebody will find a way around it one day. But they can't find a way around your backups. And, if you (and everyone else) do regular backups, you'll remove the only joy in life these worms have. They'll kill themselves, hopefully, and an entire subspecies will be wiped out -- and you'll be partially responsible!

My advance thanks for helping to exterminate these little slimebuckets.

(continued from page 27)

waiting (by dialing *70 or 1170). On the very next page is a news release from Bellcore about deluxe call waiting, which lies about the newest "multitiered" feature to suspend call waiting. As usual, the liars want to charge for a "new" feature which already exists. This is typical of the genius mind of Ma Bell. I hope that you will illustrate this abuse in your summer issue.

Also, I have mixed feelings regarding the quarterly format. But, as usual, it's worth the wait.

GH

*We actually did point that injustice out in a previous issue. While it isn't completely a lie (it seems somebody did invent something a little bit different that does basically the same thing as the old "*70"), it certainly qualifies as misleading the public.*

New Falwell Numbers

Dear 2600:

I just got ahold of the new toll-free numbers for Jerry Falwell's All Time Gospel Hour! They are 800-345-8095 and 800-453-3800.

A True Believer

It's amazing how popular these numbers are in the hacker world. We did a little checking (we called 800 info) and got 800-325-3388. Three toll-free numbers! Scary, isn't it?

What is Sprint Up To?

Dear 2600:

The very day that I received your Spring issue, I also got my Sprint bill. I read your issue first, of course, and I didn't touch my bill until I read your little blurb about Sprint's billing system in your "Happenings" column. And was I in for a surprise.

My bill was a total mess! Sprint had done two things to my bill as far as I could fathom from the mess printed on those pages. 1) They had charged me for busy signal calls. 2) They had chopped up large calls into 4 or 5 smaller calls.

I called Sprint right away and had it out with the billing person. He gave me credit for all of the one minute busy calls (about 40 altogether). As for why they did this in the first place I don't know. Is their billing computer really that messed up that they can't keep track of the status of a call? They must have a lot of this happening, because he gave

(continued on next page)

2600 LETTERS

me credit without too much of a problem.

As for the chopped up calls, that's a different matter altogether. He refused to change my billing to make the series of smaller calls into one big call. I'll have to write the company about that one.

Here is what I would like you guys to think about: We all know about those thieves who reprogram a bank's computer to shave off .00001 percent of all the accounts in the bank and drop it into another account for themselves. The small amount taken from the individual accounts will be insignificant for anyone to notice, but the total amount can be quite large. Well, here we have a long distance company that is cutting up callers' long calls into smaller calls and then charging the callers more for the first minute on all of the small calls. This amount is small and I don't really care about it. But if they're doing this to ALL callers--how much are they actually making per month?

**Cray-Z Phreaker
Skunk Works**

What you're implying here is a very serious matter. If Sprint is in fact doing this, they could be facing an awful lot of trou-

ble (something a lot of phone phreaks would no doubt relish). Let's find out for sure. Let's all put them to the test and keep logs. In fact, why not do it for all of the companies?

If you have a letter for us, send it to:

2600 Letters

P.O. Box 99

Middle Island, NY 11953

Or send it electronically using our bulletin boards or network addresses listed in our staffbox.

NORWAY BBS'S BY JOHN DRAKE

Begen Byte	5 32 02 96
Big Blue	2 42 66 88
Costa de Vindenes	5 15 16 10
DAF BBS	2 15 98 07
DASAN	3 45 95 30
Dutahyskolen	2 65 92 50
Flateby Data Klubb	2 92 89 52
Hackers Unlimited	2 24 37 40
Haugesund RBBS	4 71 40 46
HC Info BBS	3 75 45 74
Hot Stuff BBS	2 30 46 00
Modula-2 Fido	6 97 33 35

U.K. BBS'S BY JOHN DRAKE

TBBS	348 9400
London Underground	863 0198
Apple 2000	0394 276306
Apple	0268 7789565
Black Tower	474 5505
The Outer Limits	549 4845
Adult PBBS	04862 25174
444	0787 247619
Airtel	200 3439
Mac Tel	0602 455444
Mega Anchovy	747 4662
Twilight Zone (ST)	788 0884
BBS09 (ST)	0705 736025
Alternate Reality	0959 76695
	204 8755
Peoples Palace	041 956 6537
	0423 865 392
Dublin	885634

800 BBS'S

THANKS TO DENNIS FROM L.L.
AND WBAL IN NEW YORK

800-323-7464
800-365-6262

800-222-4922
800-842-5151

800-632-7227

2600 Marketplace

WANTED copied (dead) or alive! TAP'S "C" & "D" elec. courses. Cassette tape (TAP exclusive), & fact sheets #1-4. Have any or all? Contact me—willing to pay good money for orig's. B. Barton, 84 Daphne Cres., Barrie, Ontario L4M 2Y9. (705-726-6617)

WANTED: All newer hardware you find a must to quickly get rid of. Product evaluations are welcomed. Also looking for Technics SL1200 and any information related to pirate radio (including stories written by ex-pirates, groups, equipment information, FCC) for a write-up. David Jon

Hyams, E 9116
Sprague Av.,
Apt. 111,
Spokane, WA
99206

SELLING
COPIES of
A b b i e
H o f f m a n ' s
"Steal This

Book". \$7.95 + \$2 shipping & handling. Marco, P.O. Box 1211, Westerly, RI 02891.

FOR SALE: Ultimate blue box, Berry Electronics Model 312A trunk test set, has rotary dial/MF keypad, monitor speaker. Uses L-C oscillators. VERY stable. Can be used as Std phone when head/handset added. \$250. Write: Testset, 6715 Eberlein Ave., Klamath Falls, OR 97603.

WANTED: Any hacker and phreaker software for IBM compatible and Hayes compatible modem. If you are selling or know anyone who is, send replies to A.H. Moon, 25 Amaranth Crt., Toronto, ONT., Canada M6A 2P1.
WOULD YOU LIKE TO MAKE SOME MONEY? Big money? Send a business sized S.A.S.E. to: J. Duffy, 408

Michell St., Ridley Park, PA 19078. This plan is completely LEGAL.

QUALITY TAP REPRINTS. Complete set (#1-91) punched and bound. High quality copies with all special supplementals. \$75/set, shipped UPS or USPS or \$90/set shipped Federal Express. Money orders only, payable to Jeff. TZG, P.O. Box 1515, Columbus, NE 68601-1515.

WANTED: G-file "Better Homes and Blueboxing Part 2" by Mark Tabas. If anyone can provide a hardcopy, please send it to JRE, 1447 Graber Dr., Cleveland, OH 44107.

TAP BACK ISSUES, complete set Vol. 1-90 of **QUALITY** copies from originals. Includes schematics and indexes. \$100

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.

postpaid via UPS or First Class Mail. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

FOR SALE: Okidata Microline 92 personal printer. Includes manual for instructions. Hardly used. Make an offer and if it's reasonable, I will pay postage. Matt Kelly, 310 Isbell, Howell, MI 48843.

2600 MEETINGS. First Friday of the month at the Citicorp Center—from 6 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info.

Deadline for Autumn Issue: 8/31/88.

VI. KEEP YOUR ADDRESS CURRENT

To assist the Court and the parties in maintaining an accurate list of the members of the Class, please notify the Clerk of the Court of any change of address.

All Proofs of Claims, Exclusion Notices, notices of intention to appear, objections, and address corrections should be addressed to:

Clerk of the United States District Court
Eastern District of Michigan
Allnet Class Action
P. O. Box 277
Franklin, Michigan 48025

ENTERED BY ORDER OF:
Honorable Anna Diggs Taylor, Judge
United States District Court
Eastern District of Michigan
Detroit, Michigan
Clerk
United States District Court
Eastern District of Michigan
Detroit, Michigan

Dated: March 30, 1988

PROOF OF CLAIM

To participate in the settlement, you must complete this Proof of Claim and mail it (along with the address label below) to the Clerk of the United States District Court, Eastern District of Michigan, Allnet Class Action, P. O. Box 277, Franklin, Michigan 48025. **This Proof of Claim must be postmarked on or before July 28, 1988.** Please print or type.

(continued from page 2)

- 1. Name of claimant _____
Address _____
Telephone number where you can be reached during business hours (_____) _____
Name and position of person completing this form if claimant is not an individual _____
Allnet account number _____

- 2. Check here if claimant is currently an Allnet subscriber. _____
- 3. Please choose **one** of the four options listed below. Please provide the information requested.

- A. Standardized Credit or B. Standardized Cash Refund

Subject to the pro rata provisions set forth above in Section II of the Notice of Settlement, a Standardized Credit or Cash Refund equals 90 cents for each year you were a customer.

- (i) Please circle each year or part of a year in which you were an Allnet customer.

1981	1983	1985
1982	1984	

- (ii) Total number of years circled _____

- C. Itemized Credit or D. Itemized Cash Refund

Subject to the pro rata provisions set forth above in Section II of the Notice of Settlement, an Itemized Credit or Cash Refund equals 30 cents for each minute of unanswered calls for which you were charged.

- (i) Provide the following information for each unanswered call for which you were charged and have not received a prior credit or refund. This information may be provided by attaching copies of your bills with the calls circled.

<u>Date of Call</u>	<u>Area Code And Number Called</u>	<u>Number of Minutes</u>
---------------------	--	--------------------------

- (ii) Total number of minutes listed _____
- (iii) Please attach copies of the bills for each call listed. If you no longer have the bills, provide the Allnet access code to which the calls were billed, or if an access code was not used, the telephone number to which the calls were billed. _____

- 4. If you chose the **standardized credit** or **itemized credit** options, and you are not currently an Allnet customer, you must complete the following authorization form:

I authorize Allnet to notify my local telephone company that I am choosing Allnet as my Primary Long Distance Carrier on the telephone number listed below. I understand that:

- (i) If I incur a telephone company service charge in connection with the opening of my Allnet account, I will receive a credit to be applied to my Allnet account for the full amount of such service charge upon submission to Allnet, at the address to which this authorization form was sent, of a copy of the invoice for such charge
- (ii) While Allnet will be my Primary Long Distance Carrier, I will also be able to place calls with AT&T or any other carriers at any time I wish.
- (iii) I may choose only one Primary Long Distance Carrier for the listed telephone number. If I choose another carrier later on, this selection will be invalidated
- (iv) I may change to another carrier at any time, and, if I do, my local telephone company may apply a service charge
- (v) I may designate only one telephone number. The telephone number listed below is the one for which I am making this designation.

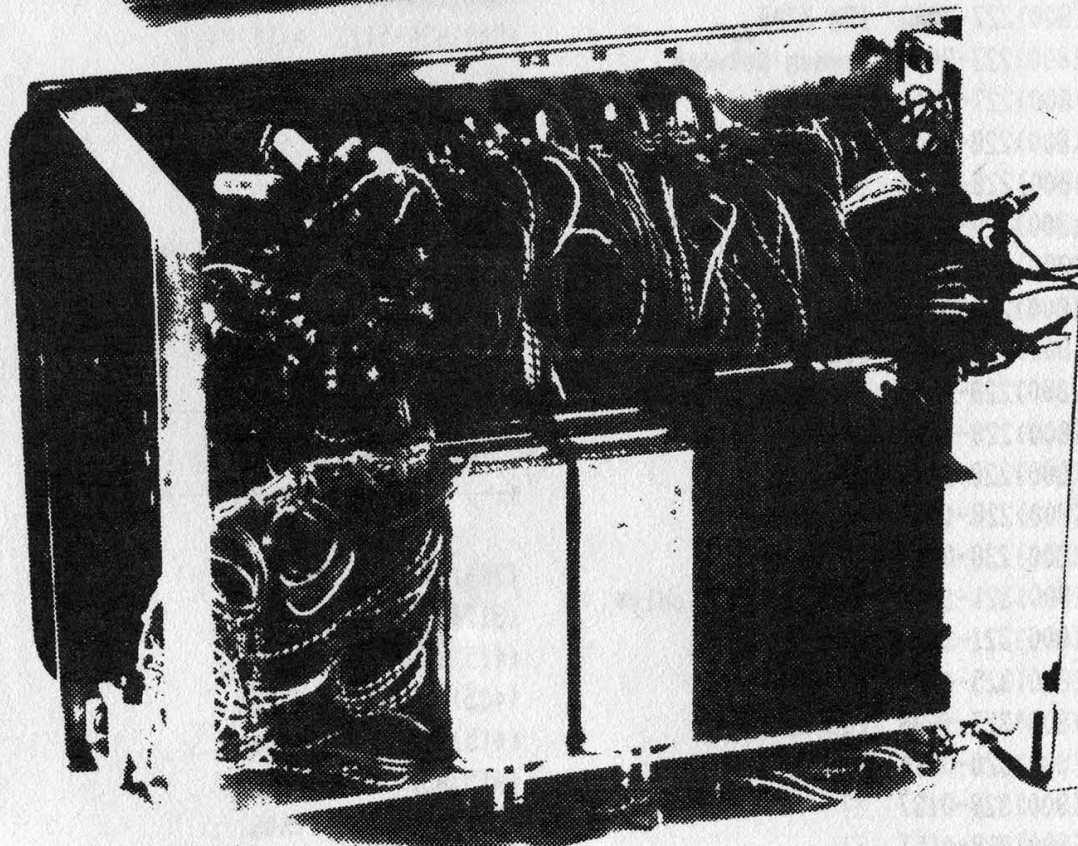
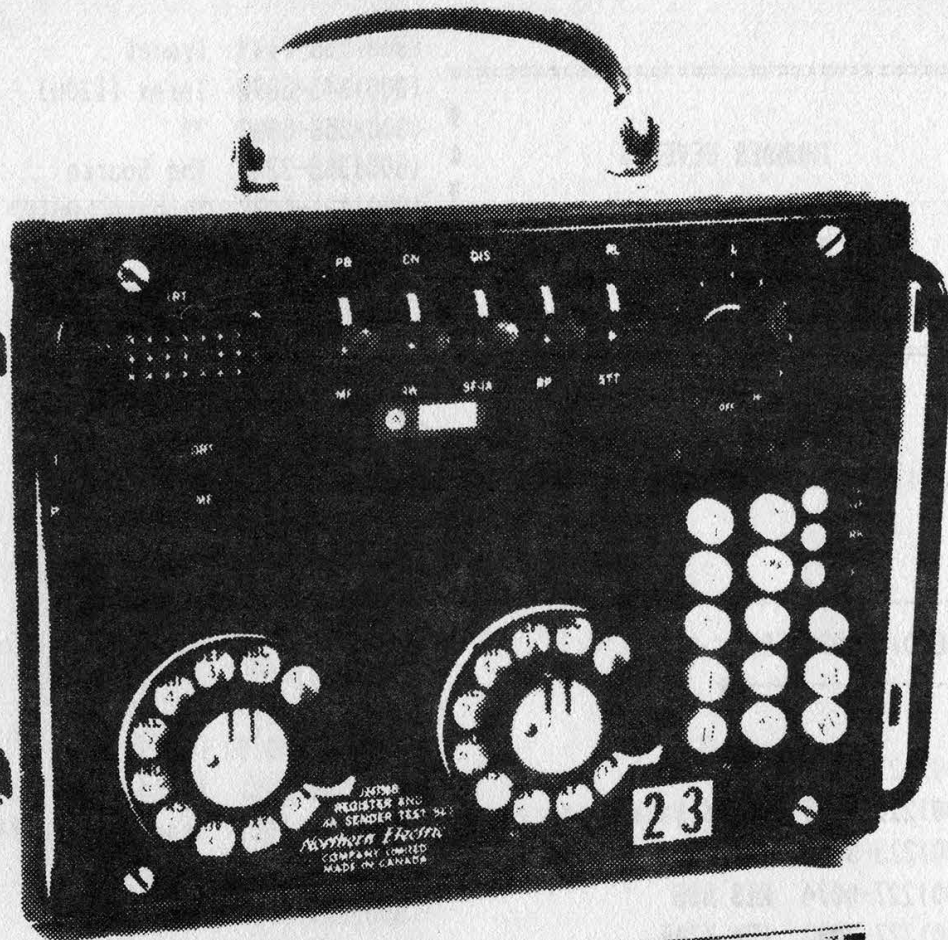
Customer name _____
 Name of billing contact (if different) _____
 Billing address _____
 Suite or apartment no. _____
 City _____ State _____ Zip _____
 Installation address (if different) _____
 Telephone number to be connected (_____) _____
 Date _____ Signature _____

CERTIFICATION AND RELEASE

I certify under penalty of perjury that I am authorized to make this claim, that the claimant was an Allnet customer at some time during the period March 2, 1981 through December 31, 1985, and that the claimant was charged for unanswered calls for which no credit or refund was previously received. I further certify that all information in this Proof of Claim is true and correct to the best of my knowledge, information and belief; that the claimant did not elect to be excluded from the Settlement Class; that the undersigned is the claimant or is authorized to execute and submit this Proof of Claim on claimant's behalf; and that this claim is the only claim being submitted in this settlement by or on behalf of the claimant.

In consideration of the right to receive benefits under the settlement, the claimant expressly covenants and agrees that he/she/it shall not now or hereafter institute, maintain or assert any claim relating to the billing of claimant for unanswered calls by Allnet during the period from March 2, 1981 through December 31, 1985. Claimant further releases all claims against Allnet, its predecessors, successors, affiliates, assigns and its officers, directors, agents and employees, past and present, that have been, might have been, are now or could be asserted in the lawsuits described in the Notice or that relate in any way to the matters alleged in the complaints in those lawsuits.

(Signature)



Photos by John Drake


```

=====
#
# THUNDER SEVEN'S
#
# List Of Numbers
# Rev. 1.0
#
=====
(800)336-0149 Tymnet
(800)345-3878 Telex [1200]
# (800)358-5880 ??
# (800)368-3343 The Source
# (800)421-0082 "please LOGIN"
# (800)421-0092 ??
# (800)424-9494 Telenet
# (800)426-2638 Soft Search
# (800)444-4472 Novell
(800)521-2255 Autonet
(800)526-3714 RCA
(800)533-5294
(800)533-5295
(800)533-5296
(800)533-5297
(800)533-5298
(800)533-5299
(800)543-0010 CINTI OH AD
(800)558-0001 Agridata
(800)621-1411 Freedom network *300 baud only*
(800)621-4243 Pathology Clc.
(800)621-9080 Datalynx
(800)624-5123 AT&T Mail
(800)638-8369 6Enie
(800)826-8855 AM. Peoplelink
(800)828-6321 XEROX
(800)847-0109 ??
(800)848-4480 Compuserve
(800)852-0005 [DIAL:]

+-----+
: (800) COMPUTERS :
+-----+

(800)222-0011 ??
(800)222-0555 World Bank Mainframe
(800)223-3312 CitiCorp
(800)227-0074 RIS BBS
(800)227-3083 IBM 3708
(800)227-3404 Bowman Network
(800)227-6544 [Unix]
(800)228-0003 ?? *300 baud only*
(800)228-0018 ??
(800)228-0329 ??
(800)228-0616 Maryland C.C.
(800)228-0748 ??
(800)228-0993 BCS
(800)228-0994 BCS
(800)228-1111 Visa (?)
(800)228-1170 ??
(800)228-1657 PHILNET
(800)238-0631 Telenet
(800)321-1646 ?? *300 baud only*
(800)321-3910 ??
(800)325-4112 Easylink
(800)327-9638 Easynet
(800)328-0024 ??
(800)328-0137 ??
(800)328-0157 ??
(800)328-0187 BWRR
(800)328-0198 ??
(800)328-4011 ??

+-----+
: VOICE MESSAGE SYSTEMS :
+-----+

(201)953-2222 VMBS
(317)267-1901 VMBS
(415)330-7831 VMBS
(415)338-7000 ASPEN
(415)463-6099 VMBS
(415)882-7170 VMBS
(703)934-3400 VMBS

800's are MUCH better...

(800)222-0311 ASPEN
(800)222-4663 VMBS

```

(800)222-5275	ASPEN	(800)759-1212	The Message Center
(800)222-9825	VMBS	(800)759-5000	Ingram Switchboard
(800)228-0368	Phone mail system	(800)777-MAIL	MCI Mail
(800)228-0464	ESAB North America	(800)824-0010	??
(800)22-VOICE	Voicebank *another dialup for 88-VOICE*		
(800)262-8477	Unisys Answering Service		
(800)284-MAIL	Meridian Mail	(800)847-6181	Western Digital
(800)323-3433	VMBS	(800)872-4634	VMBS
(800)323-3938	VMBS	(800)877-TALK	VMBS
(800)323-4222	VMBS	(800)888-0030	Receiver America
(800)323-4555	Dexter Midland	(800)888-1515	VoiceLink
(800)323-5840	Safety Claims Corp.	(800)888-MAIL	Phone Mail System
(800)323-5917	VMBS	(800)88-VOICE	Voicebank *is the same as 22-VOICE*
(800)323-8274	VMBS	(800)999-0025	Access Service
(800)325-5554	VMBS	(800)999-0085	ASPEN
(800)331-1763	Innovative Software	(800)999-TALK	ASPEN
(800)333-MAIL	Phone Mail System		
(800)342-MAIL	Phone Mail System		
(800)344-1884	VMBS		
(800)346-5104	Security Link and Telelink		
(800)423-7574	VMBS		
(800)424-3434	VMBS	(201)644-2330	("Enter first and last name...")
(800)424-6262	ITT Voice Mail System	(201)644-2332	...Call this one collect!!
(800)437-6100	Phone Mail System	(201)644-2335	News Service
(800)441-3612	VMBS	(201)644-2336	("Enter first and last name...")
(800)444-2003	VMBS	(201)644-2338	Credit Transfer/ATM
(800)445-MAIL	Phone Mail system	(201)644-2339	Automated Juror Select
(800)456-8899	Olympic Transportation	(201)644-2340	Credit Transfer/ATM
(800)521-8477	VMBS	(201)644-5621	Computerized Test
(800)524-2133	ASPEN	(201)644-5639	" "
(800)541-0641	VMBS	(201)840-9403	Bridge
(800)545-MAIL	VMBS	(202)456-1414	The White House
(800)631-1146	VMBS	(202)456-7639	Executive Office of The President
(800)654-8692	Security UN Life Insurance	(202)457-2980	Bridge
(800)662-MAIL	Voice Message Exchange	(202)457-3200	Bridge
(800)678-MAIL	VMBS	(202)457-7970	CBS News, Washington

+-----+

: Other Phun Stuff :

+-----+

NOTES: * The (201)644-XXXX numbers are only bell computerized test numbers and their functions are not actually put into effect (as far as I know).

* The status of bridges may change daily, so they may or may not be up at a given time. All the ones on here have worked recently.

* The XXXX in ringback numbers are the last 4 of your number, and you will probably have to pick up the phone and hang it up again before it rings.

* For a large list of other AT&T NewsLines, see BLOC Agent 003's BASIC TELECOM Part II, many still work.

(212)970-4747, 4848, 7272, 7979, 8080, 8686, 8787, 9090, 9494, 9898, 9999 Sex Lines
(213)617-2287 976 Backdoor
(213)617-3284 976 Backdoor (800)759-TALK Skylark
(213)935-1111 Sweep Tone Test (800)777-MEET Gay Conference Line (kill em!!) @
(214)357-8686 Sweep Tone Test (800)826-6290 Automatic Disconnect Service
(215)340-0052 Packet Switch (800)877-4700 Sprint Weather Line
(215)538-7032 Packet Switch (801)782-9699 Sweep Tone Test
(215)610-XXXX Ringback [215 NPA] (818)761-1198 Bridge
(215)698-0049 Sweep Tone Test (818)501-3400 Bridge
(215)867-1212 WZZD Weatherline 0-959-1230 Coin Test (works from some payphones)
(303)363-5929 Bridge 0-700-456-100x Alliance Teleconferencing
(312)592-6888 Bridge 10041-1-700-777-7777 Allnet Conference
(313)424-0900 Mich. Bell Automated CN/A
(313)827-7151 Bridge
(412)633-3333 AT&T Newsline, PA @ 2600 NOTE: WE THOROUGHLY DEPLORE IGNORANT
(415)284-1111 Sweep Tone Test AND PREJUDICED STATEMENTS LIKE THIS ONE
(513)375-8580 Bridge AND HOPE MOST OF OUR READERS DO TOO. WE
(513)241-8580 Bridge DECIDED TO KEEP IT IN THIS LIST TO FACE
(603)226-3949 Bridge UP TO THE FACT THAT THE HACK/PHREAK
(617)494-9900 Sweep Tone Test WORLD HAS ITS OWN REDNECK ELEMENT.
(619)375-1234 Time & Temperature
(717)255-5555 AT&T Newsline, PA
(718)528-9979 Sweep Tone Test
(800)222-TALK Consolidated Connection Talking Yellow Pages
(800)223-3331 Bank-By-Phone
(800)225-0233 Conference Operator
(800)228-0014 CC Check (hit # after tone)
(800)228-0032 CC Check (hit #)
(800)228-9901 CC Check
(800)233-3996 Discover Check
(800)257-TALK Money Talk
(800)325-5555 AT&T service report/check?
(800)327-1111 Visa/Mastercard Check
(800)433-4424 Discover Check
(800)424-5454 Fraud Hotline
(800)424-9090 White House Press Line
(800)445-3024 Sprint Operator
(800)526-3366 Jam Demo Hotline
(800)527-6178 Midas Touch Credit Check
(800)528-2121 American Express Check
(800)554-2265 Visa Check
(800)692-8766 Watson Voice Message Demo
(800)732-2255 "High Seas" Operator

Originally uploaded to:
=====

- Atlantis
- Digital Logic
- Demon Roach Underground
- The Central Office

NOTICE

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind. Simply indicate the amount enclosed and which, if any, back issues you want. Your address label should be on the back of this form.

\$15 1 year of 2600
\$28 2 years of 2600
\$41 3 years of 2600
\$40 1 year corporate subscription
\$75 2 year corporate subscription
\$110 3 year corporate subscription
\$25 overseas subscription (1 year only)
\$55 overseas corporate subscription (1 year only)
\$260 lifetime subscription (never again will we bother you)

Back issues are available. Prices are:

\$25 1984, 1985, or 1986 issues (12 per year)
\$50 Any two years
\$75 All three years (36 issues)
(Overseas orders add \$5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

**1987 ISSUES
ALSO AVAILABLE!**

AMOUNT ENCLOSED FOR SUBSCRIPTION: _____

AMOUNT ENCLOSED FOR BACK ISSUES: _____

1984 1985 1986 (circle years ordered)

TOTAL AMOUNT ENCLOSED: _____

(clip and send to us—your address is on the back)

CONTENTS

ALLNET'S LEGAL PROBLEMS.....	2
A SOLUTION TO VIRUSES.....	4
HOW TO WRITE A VIRUS	8
BUILDING A RED BOX.....	13
REPLY TO CAPTAIN ZAP	16
LETTERS	24
2600 MARKETPLACE	41
FUN PHONE NUMBERS.....	44

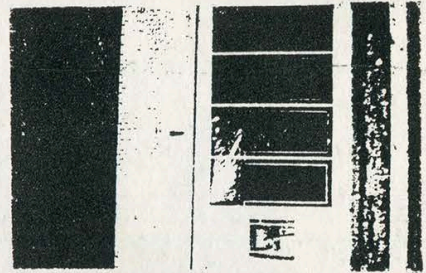
SECOND CLASS POSTAGE
Permit Pending at
East Setauket, N.Y.
11733
ISSN 0749-3851

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

DANGER:
MISSING LABEL

2600

The Hacker Quarterly



Volume 5, Number 3

Autumn, 1988





A FRENCH PAYPHONE (in France!).

Photo by John Drake

ON THE COVER:

Using a special computer language created by AT&T Bell Laboratories scientist Gerald Holzmann, two Polaroid photographs showing opposite sides of a woman's face were combined to create this image. The two 4-inch by 5-inch Polaroid photographs, through the use of an optical scanner, were digitized so they could be processed by a computer. Using his special computer language, Holzmann made a mirror image of one of the photographs, then combined the three of them to create the effect. The combination is completely seamless, revealing no discontinuities where the three photos meet -- even under magnification.

Holzmann's language and techniques are the subject of a book, Beyond Photography: The Digital Darkroom, from Prentice-Hall.

December 10, 1988

Literally for years now, we have been pestering New York Telephone for an exact date on the cutover of our ancient #5 Crossbar office to a more modern and efficient switch. And recently, we were shocked to hear that the date had been set: December 10, 1988. We thought of having a contest. A prize for the first person to call in after the cutover. But this was not to be. You see, our office is going to go

"equal access" on that date. But we're not getting a new digital switch until at least 1990. What we're getting now is something called an "adjunct frame", a device which allows a crossbar to emulate E.S.S. to a degree. Supposedly, it causes lots of problems, so we'll have something to talk about. In this way, N.Y. Tel will fulfill Judge Greene's equal access orders without spending lots of money.

STAFFBOX

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Bobby Arwatt

Cover Art
Ken Copel

Writers: Eric Corley, Thomas Covenant, John Drake, Mr. French, The Glitch, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOG, David Ruderman, Silent Switchman, Mike Yuhus, and the usual anonymous bunch.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1988, 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada -- \$15 individual, \$40 corporate.

Overseas -- \$25 individual, \$55 corporate.

Back issues available for 1984, 1985, 1986, 1987 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.

2600 Office Line: 516-751-2600

BBS #1 (OSUNY): 914-725-4060

BBS #2 (CENTRAL OFFICE): 914-234-3260

BBS #3 (YOYODYNE): 402-564-4518

BBS #4 (BEEHIVE): 703-823-6591

USENET ADDRESS: 2600@dasy1.UUCP

ARPANET ADDRESS: phri!dasy1!2600@nyu

OUTSIDE LOOP DISTRIBUTION PLANT

by Phucked Agent 04
Introduction/Outline

Basically, the outside local loop distribution plant consists of all of the facilities necessary to distribute telephone service from the central office (CO) out to the subscribers. These facilities include all wire, cable, and terminal points along the distribution path. In this article, we shall follow this path from the CO to the subscriber, examining in depth each major point along the route and how it is used. This is especially useful for checking if any "unauthorized equipment" is attached to your line, which would not be attached at the Central Office. I suppose this article can also be interpreted to allow someone to do just the opposite of its intended purpose....

Note that this article is intended as a reference guide for use by persons familiar with the basics of either LMOS/MLT or the operation of the ARSB/CRAS (or hopefully both), because several references will be made to information pertaining to the above systems/bureaus.

Serving Area Concepts (SAC) Plan

In order to standardize the way loop distribution plants are set up in the Bell System of the U.S. (and to prevent chaos), a reference standard design was created. For urban and suburban areas, this plan was called the Serving Area Concepts (SAC) plan. Basically, in the SAC plan, each city is divided into one or more Wire Centers (WC) which are each handled by a local central office switch. A typical WC will handle 41,000 subscriber lines. Each WC is divided into about 10 or so Serving Areas (depending on the size and population of the city), with an average size of 12 square miles each (compare this to the

RAND (Rural Area Network Design) plan where often a rural Serving Area may cover 130 square miles with only a fraction of the number of lines). Each Serving Area may handle around 500-1000 lines or more for maybe 200-400 housing units (typically a tract of homes).

From the CO, a feeder group goes out to each Serving Area. This consists of cable(s) which contain the wire pairs for each line in the SA, and it is almost always underground (unless it is physically impossible). These feeder cables surface at a point called the Serving Area Interface (SAI) in a pedestal cabinet (or "box"). From the SAI, the pairs (or individual phone lines) are crossed over into one or several distribution cables which handle different sections of the SA (i.e., certain streets). These distribution cables are either of the aerial or underground type. The modern trend is to use buried distribution cables all the way to the subscriber premises, but there are still a very large number of existing loop plants using aerial distribution cables (which we will concentrate mainly upon in this article). These distribution cables are then split up into residence aerial drop wires (one per phone line) at a pole closure (in aerial plant), or at a cable pair to service wire cross box (in buried plant). The cable pairs then end up at the station protector at the customer's premises, where they are spliced into the premise "inside wire" (IW) which services each phone in the customer's premises (and is also the customer's responsibility).

Although this is the "standard" design, it is by no means the only one! Every telco makes its own modifications to this stan-

OR HANDS-ON EXPERIENCE

dard, depending on the geographic area or age of the network, so it's good to keep your eyes and your mind open.

At this point, we will detail each point along the Loop Distribution Plant.

Cable Facility F1 - CO Feeder

The F1 cable is the feeder cable which originates at the Main Distribution Frame (MDF) and cable vault at the local CO and terminates at the SAI. This cable can contain from 600 to over 2000 pairs, and often more than one physical F1 cable is needed to service a single Serving Area (at an SAI). The F1 is almost always located underground, because the size, weight, and number of feeders leaving the CO makes it impossible to put them on normal telephone poles. Since it is also impractical to use one single piece of cable, the F1 usually consists of several pieces of large, pressurized, or armored cable spliced together underground (this will be covered later) into a single cable.

Cable Numbering

In order to make locating cables and pairs easier (or possible, for that matter), all of the cables in the loop distribution plant are numbered, and these numbers are stored in databases such as LMOS at the ARSB or other records at the LAC (Loop Assignment Center) or maintenance center. When trying to locate someone's cable pair, it helps a great deal to know these numbers (although it can be done without them with experience and careful observation). Probably the most common place to find these numbers is on a BOR, in the "Cable and Assignment Data" block. The F1 is usually assigned a number from 00 to 99 (although 000-999 is sometimes used in large offices). Cable *pair* number-

ing is different however, especially in older offices; typical F1 pair numbers range from 0000 to 9999. Keep in mind that the pair number is not concrete -- it is merely nominal, it can change, and it doesn't necessarily have any special meaning (in some well organized offices, however, the cables and pairs may be arranged in a certain way where you can determine what area it serves by its number...such as in my area, heh heh). In any case, it's up to you to figure out your area's layout. The cable-pair number is usually written in a format such as 02-1495, where 02 is the cable and 1495 is the pair (incidentally, since this is the CO Feeder cable pair that is connected to the MDF, it is the one that will be listed in COSMOS).

F1 Access Points

Although the F1 is run underground, there is really not a standard access point down there where a certain pair in a cable can be singled out and accessed (as will be explained next). There is, however, a point above ground where all the pairs in the F1 can be accessed -- this point is known as the Serving Area Interface (SAI), and it will be detailed later. In LMOS or other assignment records, the address of the SAI will be listed as the TErminAl Address (TEA) for the F1 cable handling a certain pair in question; therefore, it is where facility F1 stops.

Underground Plant

The term "Underground Plant" refers to any facilities located below the surface of the earth. This includes truly "buried" cables, which are located 6-or-so feet underground surrounded basically by a conduit and dirt, as well as cables placed in underground cement tunnels along with

CRAWLING INTO MANHOLES

other "below-ground" equipment (such as seen in most urban areas). Whereas the first type is really impossible to access (unless, of course, you want to dig for a day or so and then hack into an armored, jelly-filled PIC cable -- then you should take a bit of advice from our resident lcky-PIC "Goo" advisor, The Marauder), the latter type can be accessed through manholes which lead to the underground tunnel.

Manholes

Bell System manholes are usually found along a main street or area where a feeder cable group passes through. Using an underground cable location map is the best method for locating cable paths and manhole appearances, although it may not always be available. These maps can be acquired from the Underground Service Alert (USA) (at 800-422-4133), but often a "cable locator" will be dispatched instead (usually he will just mark off how far down or where you can dig without hitting a cable), so this is not a very practical method. Of course, you can always follow the warning signs on telephone poles ("call before you dig", etc.) and the spans between SAI bridging heads until you find a manhole. The F1 for the SAI nearest the manhole should be found down there along with others en route to the areas they serve.

There are several types of manhole covers, both round and rectangular. The rectangular ones are sometimes just hinged metal plates covering an underground terminal or cable closure, and these are easily opened by one person. A non-hinged one may require two people. Round manhole covers (which, by the

way, are round so that a lineman can't accidentally drop the cover down the hole) are basically all the same, except for the types known as "C" and "D" type manhole covers which utilize locking bolts (these can be removed using a standard crescent or hex socket wrench). These covers are the same as the standard "B", "A", and "SA" type covers once the bolts are removed. The best way to open a cover is to use a manhole cover lifter (i.e., Defiance Corp. PTS- 49 or B-type Manhole cover lifter), although an ordinary 3/4 - 1 inch crowbar (hook-side) can be used. Put the tool into one of the rim slots and press down on the bar until the hook is pressing up against the cover flange. Then push or lift the cover a few inches up and slide it off the hole. You can use a bent sprinkler turn-off wrench on the other side to lift up if there are two of you. You

"One must use good sense when entering a manhole."

should have no problem with two people, although it can be done alone provided you are strong enough.

Once inside, check around for any test equipment or papers which may have been left inside. Basically, there is really no pair access down there, as it is mainly a place through which the protected feeder cables are run and spliced together. These splice points are usually sealed in pressurized air and waterproof closures which protect the open splices from corro-

AND CLIMBING UP POLES

sion and ultra-violent rodent attack. If for some reason you happen to find an open splice case or a cable with its armor and sheath removed, then it may be possible (although not easy) to match color codes (see chart) and find a certain pair. You would have to strip the wire near the splice, though, and this is not recommended. Don't get the bright idea to pry open, or (worse yet) blow open a splice case, as they are often pressurized (see "manhole dangers"), and the telco will frown on your actions sooner or later. Anyway, the feeder cables generally are labelled at a point near the manhole, so it is easy to find and follow any certain cable. Because of this, the manhole access points in your neighborhood are good places to examine (and even sketch or map) the cable distribution plant in your area. This could be interesting, especially if you find a lot of recently installed groups or special service cables, etc. There could even be several types of apparatus cases containing either analog or digital carrier equipment (i.e., T1 digital or O, L, or N analog), pair gain systems, repeaters, equalizers, or loading coils (which help compensate for shunt losses caused by the parasitic capacitance between pairs in pressurized cable). A typical underground apparatus facility is the BERT (Below ground Electronics Remote Terminal). However, it's unlikely that you will find any of this special equipment down there (other than loading coils, which look like metal cylinders) unless you are in a very rural or specialized area, or you happen to be in a manhole serving an inter-office trunk span (smile here).

Manhole Dangers

One must use good sense when enter-

ing a manhole, however, especially if you don't have the right equipment. First, you could drop the cover on your foot, or get a crowbar or bent sprinkler tool (the *worst*) in the groin. Secondly, you must take precautions if you stay down long, because the atmosphere in the hole will become oxygen depleted in a matter of minutes and there may be suffocating or otherwise dangerous gases in the manhole. Third, if you tamper with nitrogen-pressurized cables or closures, a depressurization alarm signal may be set off at the maintenance center, and technicians could be sent out while you are still in the hole. It is also known that expensive electronic equipment mounted below-ground (i.e., SLC remote terminals) may be equipped with tamper alarms, and they are securely locked as well.

Serving Area Interface - SAI

The Serving Area Interface (SAI) is basically the point on the loop distribution path where the F1 feeder cable is cross-connected over into one or more F2 aerial (or buried) distribution cable. This terminal can be pole, pad, or pedestal mounted -- however, for this article, we will concentrate on the pedestal mounted cabinet as it is by far the most common (the other forms are functionally similar, anyway). These things are seen all over -- the 4-foot high gray-green "boxes". There are several names for this terminal -- technically it is called the SAI or FDI (Feeder Distribution Interface), but it is usually called a Bridging Head, Pedestal, B-Box (lineman term), or just plain "Box". The standard cabinet is the Western Electric 40-Type cabinet, and it comes in several sizes, depending on the amount of cable pairs in

(continued on page 28)

cellular update

by The Glitch

There is rising interest in the cellular scene, the retail and the free aspects of it. Here's some insight into what's going on!

Expanded Spectrum -- yes, the cellular system, designed not to be overcrowded like the earlier mobile systems, is now getting packed in some urban areas. The FCC allocated 156 more channels to the system, bringing the total number of channels from 666 to 832. All manufacturers in the current marketplace are coming out with new phones (or upgrades to older phones) to cover the new channels. Uniden has upgraded their primary line, the CP-1000, to the CP-1100. Motorola has a new line, the Mini-Tac, which is feature-packed and much smaller than their previous Dyna-Tac series. This also has 832 channels. The NEC P-9000 portable (about the size of a cordless) also has 832 channels with an available upgrade to the earlier portables. Mitsubishi had designed the radio circuits of their older model line to be able to cover extra frequencies, so all it needs is a change of software EPROMS for its upgrade. Audiovox has a new model called the BC-20 with not only 832 channel capability, but also a very useful "self-test" mode (available to service technicians) which allows full manual control of the phone, including receiving any of the 832 channels individually (for testing purposes only, of course). I do expect to see other manufacturers, such as Novatel, Oki, Hitachi (a.k.a. AT&T), Fujitsu, Panasonic, and many others.

The new channels are non-linear with the rest, with some appearing "above" the old cellular band and the rest "below" the band. Likewise, some cellular test gear

manufacturers, such as IFR, are coming out with new software upgrades to facilitate testing of the newer phones.

For the cellular system to have the ability to know if a subscriber's phone is capable of being told to move to a higher channel, the phone must somehow be able to tell the cellular switch that it can accept such a command. Fortunately, when cellular came out, there were some extra bytes in the programming to allow for this. This is called the "Station Class Mark" or SCM. It is a 4-bit binary number. Bit #1 is a "1" for 832 channels or "0" for the old 666. Bit #2 is "1" for voice-activated transmit (used as a battery saver in portables) or "0" for a mobile unit. Bits #3 and #4 identify the power class of the phone: 00=3 watts, 01=1.2 watts, 10=.6 watts, and 11 is currently undefined.

So when the phone sends out a call, it will send something to this effect:

703-591-1635 (sample phone number)
8E0F1234 (sample serial number)
1000 (sample SCM)
00 (this is the "group ID")
05 (this is the "access overload class")

Most cellular systems will not be upgrading their equipment for quite some time, or at least until they begin to get overcrowded. But come the time that they do, the cellular system will try to keep these newer phones on the upper channels when space permits so that the older cellular equipment won't have to deal with overcrowded conditions. If you are in the market for a cellular phone, don't worry about getting an older or even a newer phone with 666 channels, as I seriously doubt they will fall into obsolescence for many years to come.

WHO THE HELL WAS ALMON STROWGER, ANYWAY?

It could be fairly stated that Almon Strowger was the first phreak ever to exist. It seems he had this thing for operators....

Strowger, to begin at the beginning, was an undertaker who lived in Kansas City toward the close of the century. Accounts of his life are rather sketchy, but it does seem rather fair that he may have had something of a problem with authority. He became convinced that the Kansas City Telephone Company operators had conspired to force him out of business. They were, he thought, switching calls intended for him to his competition. When he tried to place calls himself, the operators always seemed to report nothing but busy signals and wrong numbers. Registered complaints got him nothing and nowhere. It drove Strowger to such a pitch of exasperation and inspiration that in 1889 he invented what he called the first "girl-less, cussless telephone", or more neutrally, the Automatic Switch. The dialed call was the ultimate result.

Strowger first pared the definition of phone service to a single function: connecting Party A with Party B. In the old days operators did *much* more than this. They would forward calls to someone's likely location, took messages, and advised callers whom best to call for a solution to a plumbing or medical problem. To Strowger these extra services reflected power that invited abuse. (He was not necessarily being paranoid. In the early years of phone service, there were many complaints of back-talk, biased service, and eavesdropping. Lily Tomlin's routines speak to a half-forgotten memory of those experiences.) The more things change....

Then, by substituting an automatic

switching machine for the operator, Strowger gave subscribers the power to place their own calls. In oversimplified terms, his system worked like this: A subscriber who wished to call Mr. Strowger, say, would punch a button on the phone a specific number of times. The number that would be assigned to Strowger -- 3 perhaps. Each punch would send an electrical pulse to a central office, where Strowger's switch was installed. A motor would drive the arm of the switch a number of steps around a circle corresponding to the number of times the button had been pushed. In the example here, the arm would stop at Mr. Strowger's number, the third step. The arm would stay there for the duration of the call, with the voice signals passing back and forth throughout the switch arm. When the parties hung up, the switch would reset. No matter which subscriber wished to call Mr. Strowger, the same number of pulses would make the same connection in every case.

In effect, the dial pulses replaced the operator. The pulses worked like electrical trailbreakers. They built the path to the destination phone by commanding switches to move to the proper point and freezing them in that position, thus reserving those connections for the voice signals to follow along. When the called party answered, his "Hello?" retraced the path the digits had built, back to the original caller. You now know what a step-by-step, or crossbar, office is, and although they are very rare, anyone who's ever been in one can tell you the noise from all those cross-bars moving and "ker-plunking" into position is extremely loud.

Almon Strowger Jr.
(No, not the real one)

What's Going On

Only Five Left

We've been running out of many things recently. Clean air, clean water, trees, and space, to name a few. But that's minor in comparison to the ultimate crisis facing Americans today. We've got a mere handful of unassigned area codes left. And just what the hell are we going to do when *those* are gone?

Already, plans are well underway for the splitting of the 415 (San Francisco) area code in 1992. We don't know what the new area code will be. Perhaps they'll take suggestions from the public. But there are only five possibilities left: 708, 903, 908, 909, and 917. And it's not very likely that 903 will be used since that used to be used as an area code for part of Mexico. Reassigning it could cause confusion. Theoretically, area codes 200, 300, 400, 500, and 600 could also be assigned. But those would be such nice numbers to waste. It would also be possible to assign 210, 310, 410, 510, 610, 710, 810, and 910. But we haven't heard any definites.

So what's the solution? Fortunately, there is one. But it's not going to be easy.

Beginning in July of 1995, a brand new numbering scheme will begin to take effect. On the first of that month, area codes will be liberated. They will be able to be any number they wish,

no longer having to have a one or a zero in the middle.

What it basically means is that the makeup of an area code will be as flexible as that of an exchange insofar as the number of variations that are possible. 554-556-1234 could be a phone number with area code. Don't be surprised when people start noticing how much phone numbers are starting to look like social security numbers....

The Right Choice

Bugs in computer software are being blamed for this summer's massive failures in an AT&T System 85 phone system. The customer in this case was the House of Representatives in Washington, DC. According to the Washington Post, the outages have moved mysteriously around the various House office buildings, sometimes affecting all of the 16,000 lines it ties together and sometimes only affecting one building. The \$16 million system went crazy four times in a single week.

Calling Morality

A code of practice has been established on British Telecom's Callstream network covering the content of the messages, as well as advertising and promotional material. Callstream is the equivalent of America's mass

With Phones/Computers

announcement (often 976) numbers that are creating such a stir. Callstream uses phone numbers beginning with 0898, 0077, 0066, and 0055. They are billed at higher-than-normal rates.

Here's some of what the code says: (1) Communications must not encourage or incite anyone to commit a criminal offense; create racial disharmony; contain false or misleading information; involve an unreasonable invasion of privacy; or cause outrage or gross offense by reason of sexual or violent content. (2) Communications aimed at audiences which include children must not include references to sexual practices or contain language that reasonable parents would not want their children to hear.

Speaking of reasonable parents, it is now legal for married couples to place wiretaps on their home telephones in order to catch their spouses doing nasty things like having affairs. U.S. District Judge Roy Harper says it is no longer necessary in such cases for one of the parties to know they are being recorded.

A Legend Apprehended

For eight years a man known as James Clark has been journeying back and forth across America robbing pay telephone coinboxes. Such a feat had been considered impossible, but Clark

supposedly developed a lock-picking device that no one has been able to figure out. Not only that, but he has been able to stay at least 24 hours ahead of whoever has been looking for him. Until now, that is.

Clark was arrested in late August in Buena Park, California. The 49-year-old was supposedly arrested at a house in which he was living. He was supposed to have been returned to Akron, Ohio to face charges. Security officials have said they are eager to find out his methods.

Clark had developed a kind of folk hero status among many, including the FBI. They described him as the only person in the United States capable of picking the locks on the approximately 1.8 million pay phones in America.

His annual salary from his endeavors got him about \$70,000 before taxes. (That was a joke.) An Ohio Bell security official had said, "Unless somebody gets lucky, he'll probably never get caught. He's well organized, he's smart, and he's not greedy. He only hits a few widely spaced spots each day. He's always looking over his shoulder to see if there's a police car or a telephone company vehicle." According to Pacific Bell security, Clark's ability to open the phone's coin drawer, remove the box, and close the

The World of

drawer again meant that nobody would notice what he had done until a company coin collector came around.

So another dangerous criminal is off the streets. Now if they could only find the people who keep scraping "Praise God" on every pay phone in New York City.

Mystery Hacker

Authorities are all upset about a hacker who penetrated the Jet Propulsion Laboratory's computer system in May. The mystery person managed to get into three computers in a single outing, including one belonging to the Navy. JPL says it's going to use stricter security measures, a move that could wind up costing them 4 million dollars. One of the things that JPL says is at least theoretically possible for a hacker to do on its systems is to send "bogus commands" to one of the eight unmanned interplanetary explorers they currently operate.

Almost as upsetting are the mysterious phone calls that have started pouring into Arizona-based CSC Management Corporation over the past couple of months. They made the mistake of hooking up an 800 number. Now people are calling them thinking it's a dating line, demanding money back from the

phone company, and even threatening suicide. A spokesman figures the callers think it's some kind of emergency hot line. Apparently somebody's going around putting stickers on pay phones telling people to call the number 24 hours a day which is exactly what they're doing. And the company won't change its number because then they would have to notify all of their clients, which they say would cost them even more than all of these toll-free calls they're now accepting.

AOS Happenings

You may have noticed that everyone is ranting and raving about AOS. That stands for Alternative Operator Services, which basically means that another company other than AT&T completes your AT&T calling card call from a payphone, usually without your knowledge. You become aware of the fact when your phone bill arrives and the price for the call is many times what you thought it would be. Customer owned pay phones sometimes hook into other companies and the only clue the caller has that AT&T isn't putting through the call is an operator or computer that doesn't make any reference to AT&T.

There are ways around it. You can always ask to be hooked up to an AT&T operator. If that doesn't work, you can try dialing

Technological Games

800-950-1022 (MCI) or 800-877-8000 (Sprint). Their rates are almost always lower than the AOS companies.

Once the ripoff artists get put out of business, you may actually see some good come out of all of this. International Telecharge is an AOS company that offers operators who are fluent in several languages. Micro Devices and Automatic Communications both have services where you can leave a message for an unanswered phone. They keep redialing every few minutes and when the phone is answered your message is played.

A new trade group has been formed for AOS companies called Operator Service Providers of America. About 25 of the 40 AOS companies have joined. Basically, the group calls on the companies to be more up front, to lower prices, and to not block calls to other services. Of course, all of this is voluntary.

New Call Forwarding Invention

Remote call forwarding may soon be a feature for us telephone users. Two companies in New Jersey seem to have come up with the same idea.

One of the hardest parts of remote call forwarding is communicating with the home telephone; remember, all calls are

being forwarded.

The Planum Technology Corporation of Hillside, NJ has a device that waits for two separate calls within 30 seconds. (A short ring is generated before the call gets forwarded.) The second call is interpreted as a command to disable call forwarding. The machine then dials 73 or whatever the number is in that area to disable call forwarding. The user can then call back and communicate with the machine, giving it a new phone number to call forward to.

The machine does require an access code, however it seems incredibly easy to disable someone's call forwarding. Just call twice within 30 seconds and hang up each time. It would be a good idea to add a feature that resets the call forwarding if the third "confirmation" call isn't received. And hopefully the access code is longer than two digits.

The other invention comes from Herbert Waldman of Measurement Specialties Inc., in Wayne, NJ. (This guy patented the first remote access answering machine, back in 1956!)

With this system, the caller dials his number and hangs up right after the short ring. The machine then calls the number that the calls are being forwarded to. If it gets no answer, call forwarding is disabled. The

(continued on page 42)

THE 516 AREA CODE

200 NONWORKING	TE 260 KINGBACK	320 NONWORKING
201 AREA CODE	RE 261 E NORTHPORT DMS-100	RE 321 BABYLON DMS-100
202 AREA CODE	NU 262 E NORTHPORT DMS-100	322 NONWORKING
203 AREA CODE	263 NONWORKING	RE 323 GREENPORT CROSSBAR
204 AREA CODE	RE 264 MASSAPEQUA DMS-100	RE 324 E HAMPTON CROSSBAR
205 AREA CODE	RE 265 SMITHTOWN DMS-100	RE 325 WESTHAMPTON DMS-100
206 AREA CODE	RE 266 E NORTHPORT DMS-100	NR 326 FLOKAL PARK E.S.S.
207 AREA CODE	RE 267 E HAMPTON CROSSBAR	327 NONWORKING
208 AREA CODE	268 NONWORKING	RE 328 FLORAL PARK CROSSBAR
209 AREA CODE	RE 269 E NORTHPORT DMS-100	NR 329 E HAMPTON CROSSBAR
210 NONWORKING	MU 270 FLORAL PARK E.S.S.	330 NONWORKING
TS 211 CREDIT	RE 271 HUNTINGTON CROSSBAR	RE 331 PORT JEFFERSON DMS-100
212 AREA CODE	272 NONWORKING	332 NONWORKING
213 AREA CODE	RE 273 BRENTWOOD #5 E.S.S.	333 WESTBURY
214 AREA CODE	274 NONWORKING	RE 334 WESTBURY DMS-100
215 AREA CODE	275 NONWORKING	335 NONWORKING
216 AREA CODE	276 NONWORKING	VD 336 HICKSVILLE E.S.S.
217 AREA CODE	RE 277 BAY SHORE DMS-100	337 NONWORKING
218 AREA CODE	278 NONWORKING	RE 338 WESTBURY DMS-100
219 AREA CODE	279 NONWORKING	339 NONWORKING
220 NONWORKING	280 NONWORKING	340 NONWORKING
RE 221 WANTASH CROSSBAR	RE 281 MASTIC #5 E.S.S.	341 NONWORKING
BD 222 GARDEN CITY E.S.S.	DB 282 YAPHANK #5 E.S.S.	342 NONWORKING
RE 223 FREEPORT DMS-100	RE 283 SOUTHAMPTON CROSSBAR	343 NONWORKING
BD 224 BAY SHORE DMS-100	DI 284 RIVERHEAD #5 E.S.S.	344 NONWORKING
RE 225 LINDENHURST #5 E.S.S.	RE 285 LAURELTON CROSSBAR	BO 345 YAPHANK #5 E.S.S.
RE 226 LINDENHURST #5 E.S.S.	RE 286 PATCHOGUE #1A E.S.S.	RE 346 PLAINVIEW #5 E.S.S.
VU 227 GARDEN CITY E.S.S.	RE 287 SOUTHAMPTON CROSSBAR	347 NONWORKING
BD 228 GARDEN CITY E.S.S.	RE 288 WESTHAMPTON DMS-100	RE 348 BRENTWOOD #5 E.S.S.
?? 229 GARDEN CITY E.S.S.	RE 289 PATCHOGUE CROSSBAR	RE 349 PLAINVIEW #5 E.S.S.
230 RINGBACK	TE 290 SPECIAL EXCHANGE	350 NONWORKING
RE 231 BRENTWOOD #5 E.S.S.	291 NONWORKING	RE 351 HUNTINGTON E.S.S.
ND 232 BRENTWOOD #5 E.S.S.	RE 292 HEMPSTEAD CROSSBAR	RE 352 FLORAL PARK E.S.S.
233 NONWORKING	RE 293 FARMINGDALE E.S.S.	353 NONWORKING
RE 234 BRENTWOOD #5 E.S.S.	RE 294 NINEOLA DMS-100	RE 354 FLORAL PARK #1A E.S.S.
NU 235 GARDEN CITY E.S.S.	RE 295 WOODMERE CROSSBAR	355 NONWORKING
ME 236 NINEOLA DMS-100	DI 296 GARDEN CITY E.S.S.	356 NONWORKING
VU 237 GARDEN CITY E.S.S.	297 NONWORKING	VU 357 GARDEN CITY E.S.S.
238 NONWORKING	RE 298 CATCHOGUE CROSSBAR	VU 358 FLORAL PARK E.S.S.
RE 239 FIVE TOWNS CROSSBAR	DI 299 HEMPSTEAD DMS-100	359 NONWORKING
240 NONWORKING	300 NONWORKING	RE 360 SMITHTOWN DMS-100
241 NONWORKING	301 AREA CODE	RE 361 SMITHTOWN DMS-100
RE 242 DEER PARK E.S.S.	302 AREA CODE	TD 362 NOWHERE
RE 243 DEER PARK E.S.S.	303 AREA CODE	RE 363 PATCHOGUE #1A E.S.S.
RE 244 SAYVILLE DMS-100	304 AREA CODE	RE 364 SYOSSET DMS-100
245 NONWORKING	305 AREA CODE	RE 365 MAMHASSET #5 E.S.S.
II 246 SETAUKET CROSSBAR	306 AREA CODE	NR 366 SMITHTOWN DMS-100
247 NONWORKING	307 AREA CODE	RE 367 HUNTINGTON E.S.S.
RE 248 NINEOLA DMS-100	308 AREA CODE	RE 368 E NORTHPORT DMS-100
RE 249 FARMINGDALE #5 E.S.S.	309 AREA CODE	RE 369 RIVERHEAD #5 E.S.S.
TE 250 RINGBACK	310 NONWORKING	370 NONWORKING
251 NONWORKING	TM 311 NOWHERE	RE 371 FIVE TOWNS CROSSBAR
DI 252 HEMPSTEAD DMS-100	312 AREA CODE	372 NONWORKING
VU 253 DEER PARK E.S.S.	313 AREA CODE	373 NONWORKING
VU 254 DEER PARK E.S.S.	314 AREA CODE	RE 374 WOODMERE CROSSBAR
RE 255 LYNBROOK E.S.S.	315 AREA CODE	375 NONWORKING
256 NONWORKING	316 AREA CODE	376 NONWORKING
257 NONWORKING	317 AREA CODE	377 NONWORKING
258 NONWORKING	318 AREA CODE	RE 378 FREEPORT DMS-100
VU 259 SOUTHAMPTON	319 AREA CODE	RE 379 FREEPORT DMS-100

IN DETAIL

380 NONWORKING	NW 440 SMITHTOWN	500 NONWORKING
381 NONWORKING	441 NONWORKING	501 AREA CODE
VU 382 SMITHTOWN DMS-100	442 NONWORKING	502 AREA CODE
383 NONWORKING	443 NONWORKING	503 AREA CODE
384 NONWORKING	DS 444 SMITHTOWN DMS-100	504 AREA CODE
RE 385 HUNTINGTON E.S.S.	445 NONWORKING	505 AREA CODE
386 NONWORKING	446 NONWORKING	506 AREA CODE
387 NONWORKING	VS 447 PATCHOGUE #1A E.S.S.	507 AREA CODE
VD 388 SMITHTOWN DMS-100	NW 448 SYOSSET	508 AREA CODE
389 NONWORKING	449 NONWORKING	509 AREA CODE
390 NONWORKING	TE 450 TOPS RECORDING/OPERATOR	510 NONWORKING
BO 391 FARMINGDALE E.S.S.	BU 451 SELVEN DMS-100	TM 511 NOWHERE
392 NONWORKING	452 NONWORKING	512 AREA CODE
393 NONWORKING	453 NONWORKING	513 AREA CODE
394 NONWORKING	RE 454 FARMINGDALE E.S.S.	514 AREA CODE
RE 395 MASTIC #5 E.S.S.	455 NONWORKING	515 AREA CODE
396 NONWORKING	456 NONWORKING	516 NONWORKING
397 NONWORKING	457 NONWORKING	517 AREA CODE
398 NONWORKING	458 NONWORKING	518 AREA CODE
RE 399 MASTIC #5 E.S.S.	459 NONWORKING	519 AREA CODE
400 NONWORKING	460 NONWORKING	DI 520 LEVITOWN E.S.S.
401 AREA CODE	461 NONWORKING	NY 521 GARDEN CITY E.S.S.
402 AREA CODE	RE 462 CONNACK #5 E.S.S.	522 NONWORKING
403 AREA CODE	463 NONWORKING	523 NONWORKING
404 AREA CODE	464 NONWORKING	524 NONWORKING
405 AREA CODE	465 NONWORKING	525 NONWORKING
406 AREA CODE	RE 466 GREAT NECK E.S.S.	526 NONWORKING
407 AREA CODE	RE 467 RONKONKONA #5 E.S.S.	527 NONWORKING
408 AREA CODE	NU 468 RONKONKONA #5 E.S.S.	528 NONWORKING
409 AREA CODE	469 NONWORKING	529 NONWORKING
410 NONWORKING	470 NONWORKING	530 NONWORKING
TS 411 INFORMATION	VS 471 RONKONKONA #5 E.S.S.	RE 531 FARMINGDALE E.S.S.
412 AREA CODE	RE 472 SAYVILLE DMS-100	532 NONWORKING
413 AREA CODE	RE 473 PORT JEFFERSON DMS-100	533 NONWORKING
414 AREA CODE	NR 474 PORT JEFFERSON DMS-100	534 NONWORKING
415 AREA CODE	RE 475 PATCHOGUE CROSSBAR	DI 535 NINEOLA DMS-100
416 AREA CODE	NU 476 PORT JEFFERSON DMS-100	RE 536 LYNBROOK DMS-100
417 AREA CODE	RE 477 GREENPORT CROSSBAR	RE 537 SAG HARBOR CROSSBAR
418 AREA CODE	478 NONWORKING	RE 538 HEMPSTEAD CROSSBAR
419 AREA CODE	479 NONWORKING	539 NONWORKING
RE 420 FARMINGDALE E.S.S.	TE 480 OFF BATTERY TEST	RA 540 ENHANCED DIAL-IT SERVICES E.S.S.
RE 421 HUNTINGTON CROSSBAR	RE 481 HEMPSTEAD DMS-100	RE 541 MASSAPEQUA E.S.S.
RE 422 BABYLON DMS-100	RE 482 GREAT NECK E.S.S.	BO 542 GARDEN CITY E.S.S.
RE 423 HUNTINGTON CROSSBAR	RE 483 HEMPSTEAD E.S.S.	RE 543 CONNACK #5 E.S.S.
NR 424 HUNTINGTON E.S.S.	RE 484 ROSLYN DMS-100	RE 544 E NORTHPORT DMS-100
425 NONWORKING	RE 485 HEMPSTEAD CROSSBAR	545 NONWORKING
426 NONWORKING	RE 486 HEMPSTEAD E.S.S.	RE 546 FREEPORT DMS-100
RE 427 HUNTINGTON CROSSBAR	RE 487 GREAT NECK E.S.S.	VU 547 HUNTINGTON E.S.S.
428 NONWORKING	RE 488 FLORAL PARK CROSSBAR	RE 548 RIVERHEAD #5 E.S.S.
429 NONWORKING	RE 489 HEMPSTEAD DMS-100	RE 549 HUNTINGTON E.S.S.
430 NONWORKING	490 NONWORKING	RA 550 CONFERENCE LINES E.S.S.
RE 431 LONG BEACH CROSSBAR	RE 491 DEER PARK E.S.S.	551 NONWORKING
RE 432 LONG BEACH CROSSBAR	V? 492 DEER PARK E.S.S.	552 NONWORKING
RE 433 HICKSVILLE CROSSBAR	DI 493 CONNACK #5 E.S.S.	553 NONWORKING
RE 434 BRENTWOOD #5 E.S.S.	494 NONWORKING	554 NONWORKING
RE 435 BRENTWOOD #5 E.S.S.	495 NONWORKING	TS 555 INFORMATION (+4D)
ND 436 BRENTWOOD #5 E.S.S.	RE 496 SYOSSET DMS-100	556 NONWORKING
RE 437 FLORAL PARK CROSSBAR	497 NONWORKING	557 NONWORKING
438 NONWORKING	498 NONWORKING	558 NONWORKING
439 NONWORKING	RE 499 CONNACK #5 E.S.S.	VU 559 HEMPSTEAD DMS-100

A LOOK AT EVERY EXCHANGE

DI 560 HEMPSTEAD DMS-100	620 NONWORKING	680 NONWORKING
RE 561 LYNBROOK DMS-100	RE 621 ROSLYN DMS-100	RE 681 HICKSVILLE CROSSBAR
UN 562 MANHASSET #5 E.S.S.	622 NONWORKING	VU 682 SYUSSET DMS-100
RE 563 SAYVILLE DMS-100	RE 623 FREEPORT DMS-100	BO 683 GARDEN CITY E.S.S.
NR 564 HEMPSTEAD DMS-100	KE 624 OYSTER BAY E.S.S.	DI 684 MANHASSET #5 E.S.S.
KE 565 HEMPSTEAD DMS-100	NU 625 ROSLYN DMS-100	685 NONWORKING
VU 566 HEMPSTEAD E.S.S.	RE 626 ROSLYN DMS-100	UN 686 ROSLYN DMS-100
RE 567 SAYVILLE DMS-100	RE 627 MANHASSET #5 E.S.S.	687 NONWORKING
RE 568 LYNBROOK E.S.S.	RE 628 OYSTER BAY CROSSBAR	688 NONWORKING
RE 569 WOODMERE CROSSBAR	NU 629 ROSLYN DMS-100	RE 689 SETAUKET CROSSBAR
570 NONWORKING	630 NONWORKING	690 NONWORKING
571 NONWORKING	631 NONWORKING	RE 691 MASSAPEQUA DMS-100
572 NONWORKING	NS 632 PORT JEFFERSON DMS-100	RE 692 HUNTINGTON E.S.S.
573 NONWORKING	633 NONWORKING	693 NONWORKING
DI 574 FLORAL PARK E.S.S.	634 NONWORKING	RE 694 FARMINGDALE #5 E.S.S.
RE 575 PLAINVIEW #5 E.S.S.	635 NONWORKING	695 NONWORKING
RE 576 PLAINVIEW #5 E.S.S.	636 NONWORKING	MR 696 SELDEN DMS-100
NU 577 FARMINGDALE #5 E.S.S.	7D 637 NOWHERE	697 NONWORKING
578 NONWORKING	638 NONWORKING	RE 698 SELDEN DMS-100
RE 579 LEVITTOWN CROSSBAR	NY 639 DEER PARK E.S.S.	699 NONWORKING
580 NONWORKING	640 NONWORKING	700 AREA CODE
RE 581 BAY SHORE DMS-100	641 NONWORKING	701 AREA CODE
RE 582 BRENTWOOD #5 E.S.S.	642 NONWORKING	702 AREA CODE
RE 583 FIRE ISLAND E.S.S.	RE 643 DEER PARK CROSSBAR	703 AREA CODE
RE 584 SMITHTOWN DMS-100	NU 644 GARDEN CITY E.S.S.	704 AREA CODE
RE 585 RONKONKOMA #5 E.S.S.	645 NONWORKING	705 AREA CODE
RE 586 DEER PARK CROSSBAR	646 NONWORKING	706 AREA CODE
RE 587 BABYLON DMS-100	VC 647 GARDEN CITY E.S.S.	707 AREA CODE
KE 588 RONKONKOMA #5 E.S.S.	648 NONWORKING	708 NONWORKING
RE 589 SAYVILLE DMS-100	649 NONWORKING	709 AREA CODE
590 NONWORKING	650 NONWORKING	710 NONWORKING
591 NONWORKING	651 NONWORKING	TM 711 NOWHERE
592 NONWORKING	652 NONWORKING	712 AREA CODE
RE 593 LYNBROOK DMS-100	RE 653 WESTHAMPTON DMS-100	713 AREA CODE
594 NONWORKING	RE 654 PATCHOGUE #1A E.S.S.	714 AREA CODE
RE 595 DEER PARK E.S.S.	655 NONWORKING	715 AREA CODE
RE 596 LYNBROOK E.S.S.	VU 656 GLEN COVE E.S.S.	716 AREA CODE
RE 597 FIRE ISLAND E.S.S.	657 NONWORKING	717 AREA CODE
RE 598 MASSAPEQUA DMS-100	658 NONWORKING	718 AREA CODE
RE 599 LYNBROOK E.S.S.	659 NONWORKING	719 AREA CODE
600 NONWORKING	TE 660 RINGBACK	720 NONWORKING
601 AREA CODE	RE 661 BABYLON DMS-100	721 NONWORKING
602 AREA CODE	662 NONWORKING	RE 722 RIVERHEAD #5 E.S.S.
603 AREA CODE	DI 663 GARDEN CITY E.S.S.	723 NONWORKING
604 AREA CODE	664 NONWORKING	RE 724 SMITHTOWN DMS-100
605 AREA CODE	RE 665 BAY SHORE DMS-100	RE 725 SAG HARBOR CROSSBAR
606 AREA CODE	RE 666 BAY SHORE DMS-100	RE 726 SOUTHAMPTON CROSSBAR
607 AREA CODE	RE 667 DEER PARK CROSSBAR	RE 727 RIVERHEAD #5 E.S.S.
608 AREA CODE	RE 668 MONTAUK #5 E.S.S.	RE 728 HAMPTON BAYS CROSSBAR
609 AREA CODE	RE 669 BABYLON DMS-100	729 NONWORKING
610 NONWORKING	670 NONWORKING	730 NONWORKING
TS 611 REPAIR	RE 671 GLEN COVE E.S.S.	RE 731 LEVITTOWN CROSSBAR
612 AREA CODE	672 NONWORKING	RE 732 SELDEN DMS-100
613 AREA CODE	RE 673 HUNTINGTON E.S.S.	UN 733 HICKSVILLE CROSSBAR
614 AREA CODE	RE 674 GLEN COVE E.S.S.	RE 734 CATCHOGUE CROSSBAR
615 AREA CODE	675 NONWORKING	RE 735 LEVITTOWN CROSSBAR
616 AREA CODE	RE 676 GLEN COVE E.S.S.	RE 736 SELDEN DMS-100
617 AREA CODE	NU 677 SYUSSET DMS-100	RE 737 RONKONKOMA #5 E.S.S.
618 AREA CODE	KE 678 LYNBROOK DMS-100	738 NONWORKING
619 AREA CODE	RE 679 WANTAGH E.S.S.	VU 739 MINEOLA DMS-100

IN 516

740 NONWORKING	800 AREA CODE	860 NONWORKING
RE 741 MINEOLA DMS-100	801 AREA CODE	861 NONWORKING
RE 742 MINEOLA DMS-100	802 AREA CODE	RE 862 SMITHTOWN DMS-100
743 NONWORKING	803 AREA CODE	863 NONWORKING
RE 744 SHUREHAM CROSSBAR	804 AREA CODE	RE 864 LOMPAUK #5 E.S.S.
NR 745 GARDEN CITY E.S.S.	805 AREA CODE	865 NONWORKING
RE 746 MINEOLA DMS-100	806 AREA CODE	866 NONWORKING
RE 747 MINEOLA DMS-100	807 AREA CODE	NR 867 FREEPORT DMS-100
748 NONWORKING	808 AREA CODE	RE 868 FREEPORT DMS-100
RE 749 GREENPORT CROSSBAR	809 AREA CODE	RE 869 MANHASSET #5 E.S.S.
750 NONWORKING	810 NONWORKING	870 NONWORKING
RE 751 SETAUKET CROSSBAR	811 NONWORKING	871 NONWORKING
RE 752 FARMINGDALE E.S.S.	812 AREA CODE	RE 872 LYNBROOK DMS-100
NR 753 FARMINGDALE E.S.S.	813 AREA CODE	RE 873 MINEOLA DMS-100
RE 754 E NORTHPORT DMS-100	814 AREA CODE	NR 874 MASTIC #5 E.S.S.
NU 755 FARMINGDALE #5 E.S.S.	815 AREA CODE	875 NONWORKING
RE 756 FARMINGDALE E.S.S.	816 AREA CODE	RE 876 WESTBURY DMS-100
RE 757 E NORTHPORT DMS-100	817 AREA CODE	RE 877 MINEOLA DMS-100
RE 758 PATCHOGUE #1A E.S.S.	818 AREA CODE	RE 878 MASTIC #5 E.S.S.
RE 759 GLEN COVE E.S.S.	819 AREA CODE	70 879 NOWHERE
760 NONWORKING	TE 820 SPECIAL EXCHANGE	880 NONWORKING
761 NONWORKING	RE 821 SHUREHAM CROSSBAR	881 NONWORKING
762 NONWORKING	RE 822 HICKSVILLE CROSSBAR	882 NONWORKING
RE 763 LYNBROOK E.S.S.	UN 823 HEMPSTEAD DMS-100	RE 883 PORT WASHINGTON CROSSBAR
RE 764 LYNBROOK E.S.S.	DI 824 HEMPSTEAD DMS-100	RE 884 BABYLON DMS-100
RE 765 CUTCHOQUE CROSSBAR	825 WANTAGH	885 NONWORKING
RE 766 LYNBROOK E.S.S.	RE 826 WANTAGH CROSSBAR	NR 886 LONG BEACH
RE 767 PORT WASHINGTON #5 E.S.S.	827 NONWORKING	RE 887 LYNBROOK DMS-100
768 NONWORKING	828 NONWORKING	RE 888 BABYLON DMS-100
769 NONWORKING	RE 829 GREAT NECK E.S.S.	RE 889 LONG BEACH CROSSBAR
770 NONWORKING	830 NONWORKING	TE 890 TEST EXCHANGE
771 NONWORKING	831 NONWORKING	891 NONWORKING
772 NONWORKING	832 WESTBURY	892 NONWORKING
NR 773 GREAT NECK E.S.S.	833 NONWORKING	SP 893 BABYLON DMS-100
774 NONWORKING	834 NONWORKING	894 NONWORKING
RE 775 FLORAL PARK #1A E.S.S.	835 NONWORKING	895 NONWORKING
776 NONWORKING	836 NONWORKING	896 NONWORKING
777 NONWORKING	837 NONWORKING	897 NONWORKING
778 NONWORKING	838 NONWORKING	898 NONWORKING
779 NONWORKING	839 NONWORKING	899 NONWORKING
780 NONWORKING	840 NONWORKING	900 AREA CODE
RE 781 WANTAGH E.S.S.	841 NONWORKING	901 AREA CODE
782 NONWORKING	RE 842 LINDENHURST #5 E.S.S.	902 AREA CODE
RE 783 WANTAGH E.S.S.	843 NONWORKING	903 NONWORKING
784 NONWORKING	UN 844 FARMINGDALE E.S.S.	904 AREA CODE
RE 785 WANTAGH E.S.S.	NR 845 FARMINGDALE E.S.S.	905 AREA CODE
786 NONWORKING	846 NONWORKING	906 AREA CODE
787 NONWORKING	VU 847 FARMINGDALE E.S.S.	907 AREA CODE
RE 788 FISHERS ISLAND STEP BY STEP	848 NONWORKING	908 NONWORKING
RE 789 LINDENHURST #5 E.S.S.	849 NONWORKING	909 NONWORKING
790 NONWORKING	850 NONWORKING	910 NONWORKING
RE 791 WOODMERE CROSSBAR	851 NONWORKING	TS 911 POLICE EMERGENCY
792 NONWORKING	852 NONWORKING	912 AREA CODE
793 NONWORKING	853 NONWORKING	913 AREA CODE
RE 794 GARDEN CITY E.S.S.	854 NONWORKING	914 AREA CODE
RE 795 MASSAPEQUA DMS-100	855 NONWORKING	915 AREA CODE
RE 796 LEVITTOWN CROSSBAR	856 NONWORKING	916 AREA CODE
NR 797 MASSAPEQUA DMS-100	857 NONWORKING	917 NONWORKING
RE 798 MASSAPEQUA DMS-100	858 NONWORKING	918 AREA CODE
RE 799 MASSAPEQUA E.S.S.	UN 859 BAY SHORE DMS-100	919 AREA CODE

516 AREA CODE

920 NONWORKING
 RE 921 SYOSSET DMS-100
 RE 922 OYSTER BAY CROSSBAR
 923 NONWORKING
 RE 924 YAPHANK #5 E.S.S.
 925 NONWORKING
 926 NONWORKING
 927 NONWORKING
 RE 928 PORT JEFFERSON DMS-100
 RE 929 SHOREHAM CROSSBAR
 930 NONWORKING
 RE 931 HICKSVILLE E.S.S.
 VU 932 HICKSVILLE E.S.S.
 NR 933 HICKSVILLE E.S.S.
 NB 934 HICKSVILLE E.S.S.
 RE 935 HICKSVILLE E.S.S.
 936 NONWORKING
 RE 937 HICKSVILLE E.S.S.
 RE 938 HICKSVILLE CROSSBAR
 BU 939 HICKSVILLE E.S.S.
 940 NONWORKING
 RI 941 SETAUKET CROSSBAR
 NU 942 HICKSVILLE E.S.S.
 VD 943 HICKSVILLE E.S.S.
 RE 944 PORT WASHINGTON CROSSBAR
 945 NONWORKING
 946 NONWORKING
 947 NONWORKING
 948 NONWORKING
 949 NONWORKING
 TS 950 LONG DISTANCE DIALUPS
 951 NONWORKING
 952 NONWORKING
 V6 953 RIVERHEAD E.S.S.
 7D 954 NONHERE
 CH 955 DEER PARK & SELDEN E.S.S.
 956 NONWORKING
 RE 957 LINDENHURST #5 E.S.S.
 TE 958 NUMBER IDENTIFICATION
 TE 959 TEST EXCHANGE
 960 NONWORKING
 961 NONWORKING
 962 NONWORKING
 963 NONWORKING
 964 NONWORKING
 965 NONWORKING
 966 NONWORKING
 967 NONWORKING
 RE 968 BAY SHORE DMS-100
 969 NONWORKING
 970 DIAL-IT SERVICES E.S.S.
 971 NONWORKING
 972 NONWORKING
 973 NONWORKING
 974 NONWORKING
 975 NONWORKING
 RA 976 DIAL-IT SERVICES CROSSBAR
 977 NONWORKING
 978 NONWORKING
 RE 979 SLIHTOWN DMS-100

980 NONWORKING
 RE 981 KUNKUNKUMA #3 E.S.S.
 982 NONWORKING
 983 NONWORKING
 984 NONWORKING
 985 NONWORKING
 986 NONWORKING
 NW 987 SETAUKET
 988 NONWORKING
 989 NONWORKING
 990 NONWORKING
 991 NONWORKING
 992 NONWORKING
 993 NONWORKING
 994 NONWORKING
 995 NONWORKING
 996 NONWORKING
 RE 997 WESTBURY DMS-100
 998 NONWORKING
 999 NONWORKING

??=unknown use
 BU=business only
 CH=choke lines for mass dialing
 DB=Brookhaven National Labs DID
 DI=Direct Inward Dial (DID)
 DS=SUNY Stony Brook Hospital DID
 MA=mass announcements
 MC=Metro One cellular dial-ins
 NB=new, business lines only
 NU=new, DID
 NK=new, residential service
 NS=new, SUNY Stony Brook DID
 NU=new, unused
 NW=no longer working
 NY=NYNEX Mobile/Cellular dial-ins
 RE=regular residential service
 RI=numbers are duplicated in 751
 SP=sparingly populated
 TE=telco use
 TS=telephone company service
 TW=two and a half busy's after 3D
 UM=unused
 V?=very new, unknown use
 VB=very new, business lines only
 VC=very new, cellular dial-ins only
 VD=very new, DID
 V6=very new, Grumman Corporation DID
 VS=very new, sparsely populated
 VU=very new, unused
 XI=old SUNY centrex being phased out

936 and 999 were former dial-it mass announcement services. 903 was a former area code for Mexico. 233 was an unconfirmed former exchange for Selden. 440 plus any four digits used to connect to police emergency (911).

In the 516 area, it's currently not necessary to dial a one before any calls. This makes scanning it easier. In other area codes, 1 plus a number may do something entirely different than the same number without a 1 in front of it. Because 516 doesn't require a 1, it's impossible for any number that is an area code to also be used as an exchange.

This scan was done from our office in the 751 exchange. We believe it to be at least 90 percent accurate. If you know of any corrections, please forward them to us. In cases where we were not absolutely certain if an office was a #5 E.S.S., a #1A E.S.S., or a DMS-100, the generic term "E.S.S." is printed.

If you wish to do a similar scan from your area code, we would be happy to print the results. But you must be thorough. First, go through your phone book and mark down where each exchange is listed as being from. If your phone book doesn't list every exchange in your area code, you'll have to find the other books. This list of locations is NOT the location of the central offices. Getting that will take some engineering and ingenuity on your part.

Sometimes test numbers exist that identify the location and type of a central office (around here it's xxx-9901). You must also be able to tell the difference between generic E.S.S. and crossbar. 516-751-9970 is a crossbar busy. 516-360-9970 is an E.S.S. busy. But 516-423-9970 is a crossbar busy, even though it sounds very much like an E.S.S. busy. You can tell because the relays click on both sides of the busy. An electronic or digital switch has no relays and therefore doesn't click.

Once you have a list of valid exchanges and where they come from, you must see what all of the OTHER exchanges that don't exist do when you dial them. If your area code requires a 1 before some calls, you must try each and every exchange with and without a 1. This is how you find interesting features.

The final step is to see if the exchanges you have logged actually show up in the phone book. If not, odds are they are being used only by businesses or as a Direct Inward Dial (DID) for a large corporation or institution. DID's contain many beepers, fax machines, computers, etc.

Two copies of this list, one sorted by exchange and the other sorted by central office name, can be found on 2600 bulletin boards.

ANNOUNCING THE NEW PARTY LINE SERVICES

THE SAFE WAY TO MEET NEW PEOPLE, MAKE NEW FRIENDS OR JUST LISTEN IN FOR THE FUN OF IT.

JUST 11¢ A MINUTE

TRY THESE NUMBERS:

(20¢ 1st Min., 10¢ Each Add'l.)

550-LOVE
THE MEETING PLACE FOR
LONG ISLAND ADULTS

550-WILD
WHERE CITY PEOPLE COME
TOGETHER (ADULTS ONLY)

550-SOUL
FOR THE "UPTOWN
EXPERIENCE" (ADULTS ONLY)

550-ROCK
WHERE TEENS MEET AND
PARTY BY PHONE

FOR EXCITING PARTY LINE NEWS CALL 540-3733 FOR JUST \$1.50



© 1988 A.T.N.

BROUGHT
TO YOU
THROUGH
NEW YORK
TELEPHONE

NOW THEY'RE SENDING US POSTCARDS!

We especially enjoyed the New York Telephone "logo" they came up with. They won't get sued for that!

memorandum

Serial: [redacted] 163-86

DATE: 10 November 1986

REPLY TO
ATTN OF: [redacted]

SUBJECT: Unauthorized Access of DOCKMASTER - INFORMATION MEMORANDUM

TO: DISTRIBUTION [redacted]
THRU: [redacted]

Received in [redacted]
on 17 NOV 1986

1. On 25 and 31 October 1986, there were successful unauthorized accesses to DOCKMASTER. The following information has been gathered to date:

a. The connection to DOCKMASTER was made from a location in France via the Telenet network. Telenet has determined the network address of the connection point and has requested Transpac, Telenet's European counterpart, to determine the identity of the foreign host.

b. The chronological order of events is as follows:

10/25/86 09:56

Successful access was made to DOCKMASTER from France. The user was disconnected at 10:01 due to Telenet/Transpac communication problems.

10/31/86 09:50

Successful access was made to DOCKMASTER from France.

10/31/86 10:20

The owner of the account was denied access to DOCKMASTER when he attempted to login because the account was already active. The user promptly notified his project administrator, [redacted], who notified the DOCKMASTER system administration personnel.

10/31/86 10:27

User was bumped from the system and the userid locked.

10/31/86 13:35

Two attempts from France were denied due to the locked userid.

c. The user's password was last changed on 28 August 1986. There were no bad password attempts against this user since April, indicating that the user's password was not guessed, but compromised.

2. ~~The user of the account which was compromised works for Prime and is registered on the Prime project. It was determined that the unauthorized user had looked at the user's mailbox and attended the Prime reevaluation team forum which contains Prime's Proprietary information.~~ Since the unauthorized user was logged

OPTIONAL FORM NO. 10
(REV. 1-80)
GSA FPMR (41 CFR) 101-11.6
5010-114


* GPO : 1985 O - 461-275 (428)

onto DOCKMASTER for 30 minutes on 31 October 1986, it is possible that a substantial amount of proprietary information was compromised. Based on the 30 minute login time and a maximum data transfer rate of 240 characters per second, the user could have transferred up to 422 KB of data (30min * (60 sec/min) * (240 char/sec)).

3. This compromise could not have been prevented by the use of AIM (DOCKMASTER's implementation of Mandatory Access Control) since the userid which was compromised had valid AIM access to the data. The use of a separate authentication/identification device, such as the Sytek Passport, could have prevented this access. We are currently working on purchasing the Sytek.


Chief,

DISTRIBUTION

/SCSC
Chief,
D/Chief,
C Chief Scientist
Chief,
D/Chief,


reprinted from w.o.r.m. 1.5

NOTES

DOCKMASTER is the NSA's computer system hooked up to ARPANET. Its Telenet address is 30122 (NUI required). On INTERNET it is "DOCKMASTER.ARPA". I am still waiting for additional FOIA documents but the NSA has asked for \$3,400 to continue looking.

RED BOX TUNES
FOR A COMMODORE-64
WRITTEN IN BASIC
BY TUMMY

```
10 s=54272:pokes+6,240:pokes+4,32:  
    pokes+24,15:pokes+13,240:pokes+11,32  
20 pokes,229:pokes+1,140:pokes+7,239:pokes+8,108  
30 goto500  
40 rem *** quarter tone code  
50 fori=1to5:pokes+4,33:pokes+4+7,33  
55 pokes+4,32:pokes+4+7,32  
60 forj=1to25:next:nexti:return  
63 for j=1to25  
99 rem *** dime tone code  
100 fori=1to2  
110 pokes+4,33:pokes+4+7,33  
120 forj=1to30:next  
130 pokes+4,32:pokes+4+7,32  
140 forj=1to35:next  
150 nexti  
160 return  
199 rem *** nickel tone code  
200 pokes+4,33:pokes+11,33  
210 fori=1to30:next  
220 pokes+4,32:pokes+11,32  
230 return  
499 rem *** menu code  
500 print"red box tones: q for quarter"  
501 print"                d for dime"  
502 print"                n for nickel"  
510 getx$:ifx$=""then510  
520 ifx$="q"thengosub50  
530 ifx$="d"thengosub100  
540 ifx$="n"thengosub200  
550 goto510
```

 **
 ** Tommy's Canadian WAIS Phonebook **
 **
 ** Compiled July, 1988 **
 **
 ** Most numbers listed are available **
 ** Canada-wide, ALL can be reached **
 ** from the 604 NPA... **
 **

800-227-8933 KOLM
 800-227-4004 KOLM
 800-328-9632 FAX/Voice Mail System
 800-663-5000 FAX/Voice Mail System
 Hold Music = LHM-FM
 Vancouver, B.C.
 800-268-4500 Voice Mail System dialup
 800-268-4501 KOLM
 800-268-4505 Voice Mail System
 800-268-7800 Voice Mail??/
 800-268-7808 Voice Mail
 800-387-2097 voice mail/FAX
 800-387-2098 Voice Mail/FAX
 800-663-5796 Voice Mail (let ring 5)
 800-387-8803 KOLM
 800-387-8861
 8862
 8863
 8864 All the same KOLM
 800-387-8870
 8871 KOLM
 800-426-2638 Carrier
 800-647-6181 voice Mail
 800-524-2133 ASPEN
 800-268-6364 National Data Credit Check
 800-387-9115
 9116 both same ASPEN
 800-387-9173 Hold Music = LHM-FM
 Barrie, Ontario
 800-387-9218 "voice Messenger"
 800-387-9644 Carrier

1154
 THANKS TO NUMBER SEVEN AND TELECOM CANADA FOR ASSISTANCE IN COMPILING THIS

FULL FREE DIALPAD DIALUPS:
 604.....800-663-1911
 204 306 403.....800-667-7133
 204 306 406 416 519 604
 /02 80/.....800-667-8144
 416 418 506 514 519 616
 /03 80/ 619 902.....800-268-8733
 416 519 613 /05.....800-268-9200
 418 514 819.....800-463-5333
 506.....800-227-9507
 506 /03 902.....800-563-0764

LETTERS

The Schematic

Dear 2600:

I really enjoyed the article in your Summer 88 issue, "Building a Red Box". I wish and hope in future issues you publish more circuits on boxes and the sort. I'm really glad you printed the parts list because I can't read half of the components on the layout on page 23. I understand how in the condensing and trying to make it fit on an 8 1/2" x 5 3/4" page along with text, etc. What I'm getting at is could you send me an enlarged and *clear* copy of the red box plans? I would greatly appreciate it. I hope you aren't like most other dumb-ass mags and don't reply. I realize you get a lot of mail, so do the best you can. To make it easier, I've enclosed a SASE. I just want to add that your magazine is great!

The Bug Brother #1

We're sorry about the mess-up regarding the schematic. Anyone who still needs an enlarged copy of that page should either write to us or call us at (516) 751-2600. In either case, give us your subscriber number.

The Virus

Dear 2600:

Just a note to say thanks for keeping a level head in a warped world. Your publication is well worth waiting three months for. Unfortunately, I am a rather impatient sort and also a recent subscriber so I am enclosing a request for the back issues from the past three years. That should keep this inquiring mind busy for some time to come. Also I want to offer my applause regarding the article "The Dark Side of Viruses". Having read too many articles concerning how awful viruses are, yours was such a breath of fresh air. It was a repugnant, putrid blast of air to be sure but it came from an angle that was so different from the masses that it was indeed refreshing. I suspect that T. Plague was rather brutally mistreated as a child. I cannot imagine complete amorality such as his without some form of trauma. I do agree on certain aspects of his dissertation such as the need for frequent backups and his lack of respect for program pirates. He is a bit of a hypocrite though (to go along with the rest of his conditions); after all, his program does its best to circumvent even the safety of frequent backups. I also don't think it is quite his

AND A FEW NUMBERS

place to judge program pirates. Quite frankly, he is not balanced enough to weigh properly anybody's guilt or innocence. It's too bad since he is obviously not an idiot or a fool. Nor do I feel that he should be pitied. He does not deserve my or anybody's pity. Nonetheless, though I obviously do not agree with Mr. Plague's article, I did learn a lot from it. It showed a rare insight into the mind of the virus generator, the serial killer, the child molester, or the arsonist. Take your pick. The lack of remorse or simple morals and the feelings of validity of their actions seem to be prevalent in all these people. I would like to feel that Mr. Plague would resent being equated to a child molester, but he probably doesn't. Most of his prey is just as innocent and helpless as a child. He is just as guilty of taking advantage of these same attributes existent in a novice computer user.

In any case, I am looking forward to reading three years worth of wonderful, controversial, and informative articles. Keep up the good work.

Jonathan Porath

Dear 2600:

I very much appreciated the issue on viruses. I think it is a

bad thing to do if someone really destroys data other than in his own computer, but the phenomenon of spreading a virus automatically fascinates me and I think it does for a lot of people. It would be better if those who write viruses would program them not to destruct, but to play a tune, print silly messages, or to do similar things once they are activated. Furthermore, these viruses should be tested thoroughly before spreading, to avoid erasure of data. Of course, a virus should delete itself after a while from the infected program, as in real life a flu gets cured, even when you do nothing to cure it.

**Greetings from the
Netherlands
Paul van Hattum**

Dear 2600:

My God, man, *fifteen pages* were given to an article which does essentially nothing but rag on virus writers and promote a piece of software. That's almost twice as many pages as there once was in the whole mag! If I write a shareware virus protection program, can I have fifteen pages to hype it in too? As for the actual message in that article, why on earth should I trust Ross M. Greenberg after he has basical-

AUTUMNAL

ly scared me into trusting no one? Let alone send him ten clams? I'll protect my *own* goddam data, thank you very much.

Aside from too few articles that ramble on too much, 2600 is still a fine publication. I especially found the red box article helpful, as well as Thunder Seven's number list.

**Tommy
Sysop, THC-|| BBS,
6045950085**

P.S. ANI in the 604 NPA varies from CO to CO, but is usually 211 or 116. In some step or x-bar exchanges, it's necessary to put a 1 in front of that.

P.P.S. Anyone else work with 4Tel? 604-381-3717 has one of these versatile line test boxes on it...

The Chip

Dear 2600:

I wish I knew where these rumours start, but the ICL8038 is still being produced by GE Solid State (formerly called GE/RCA/Intersil). GE Solid State has many regular dealers in both the U.S.A. and Canada. Never mind that the 8038 is also handled by most electronic surplus component dealers. In addition, the 8038 is also manufactured by a company called EXAR, who makes it under their part numbers

XR8038CP, XR8038P, XR8038ACP, and XR8038AP. EXAR also has many dealers throughout the U.S.A. and Canada. By the way, EXAR is also the manufacturer of the other two most popular blue box chips; the XR2207 and XR2209.

I don't understand why people will pay 8 or up to 15 dollars apiece for these chips through private ads when they are available everywhere for around 4 dollars each.

**Rubber Soul
Toronto, Canada**

Apparently, you've never heard of designer chips, have you?

Another ANI

Dear 2600:

The ANI for the 213 area code (Los Angeles) is 61056.

The Soldier

Congratulations. We've also heard that parts of 213 respond to 1223 for a read-back of your phone number. In sections of 213 served by GTE, 114 seems to work. Others we've gotten word of are 290 for parts of Illinois, 200-xxx-xxx for other parts of Illinois, 760 for the 408 area code, 300-xxx-xxx in some areas, 711 in parts of 919, 970-xxx in parts of Texas served by GTE, 997-555-1212 in area code 502, 200-222-2222 in

LETTERS

area codes 313, 616, 906, and 517, 191# in DMS-100 switches, 990 in the 914 area, and 958 in the New York metro area. If you find an ANI, send it in to us!

BLV Tidbits

Dear 2600:

I've been doing some research on Busy Line Verification (BLV). If you remember, BLV is the technical name for an emergency interrupt. The information I have pertains to an AT&T TSPS or inward operator.

An operator cannot make an emergency interrupt without having a customer on hold, with one exception. There is a procedure known as a service test call used to check if the BLV circuits within a TSPS switch are functioning properly. This test is done *without anyone* on hold, but every time it is done a message prints on the security printer.

There is a feature which prints call detail for any emergency interrupt which exceeds a preset period of time on the security printer. The threshold can be anything from 0 to 255 seconds. Multiple interrupts on the same call are accumulated, but time when the interrupted party is on hold is not.

The tone generator, which beeps when an operator breaks

in on the line, makes a tone of 440 Hz at a -13 dBm 0 level. The first tone is 2 seconds and every 10 seconds there is a half second burst.

A TSPS's verification network is limited to 8 NPA's. A maximum of 800 local offices in each NPA can be served by a TSPS for verification (that seems like a lot to me).

BOC's have the capability to exclude telephone numbers and even whole offices from verification.

The BLV trunk group is always trunk group number 35 in every TSPS office (I thought that was neat).

Unfortunately, AT&T has stopped doing emergency interrupts in many areas, recently, due to local operators.

The Zeppelin

What's the Point?

Dear 2600:

This letter won't do any good, but I will write it anyway.

I called several of the BBS's you have listed. After a while, I hung up. I don't have time to screw with them. What is the point? Are the users frustrated hackers?

I call a lot of BBS's and they are easy to use. My time is too valuable to waste, and even more so when it is long distance to learn some stupid system just to use a silly BBS.

(continued on page 43)

OUTSIDE LOOP

(continued from page 7)

the Serving Area. The size and style of the cabinet is usually stenciled or marked on the cement pedestal at the base of the cabinet (i.e., S-40-E = 40 type, E size, SAI cabinet). These cabinets can handle anything from 400 (A size -- 200 feeder in, 200 distribution out - 43"H x 15"W x 12"D) to 1800 (E size - 900 in, 900 out - 54"H x 40"W x 12"D), with some newer size F, H, and some 3M series -- 4200 cabinets handling up to 3600 pairs at one site! Also note that 40-type (or look-alike) cabinets are not exclusively for use as an SAI, especially in areas using a buried F2 distribution plant. Note that all Bell System (Western Electric) cabinets, cross-boxes, etc. which are pedestal mounted are painted a standard grey-green. (Technically, they are painted per Munsell Color Code Standard, EIA RS-359. This color is supposed to be the least obtrusive and most pleasing to the eye.) This also helps to distinguish telco boxes from sprinkler and signal control boxes. Also note that there are still a large number of older loop plants in the Bell System, and the terminal boxes may differ (i.e., nut-bolt type binding posts, panel-removal type cabinets, etc.) in appearance, but they are all functionally similar.

To open a 40-type or other common cabinet, one must use a 7/16" hex wrench (also called a "can-" or "216-" tool). Place the wrench on the bolt and turn it 1/8 of a turn clockwise (you should hear a spring release inside). Holding the bolt, turn the handle all the way to the right and pull the door outward. If you happen to see a locked cabinet pried open by a crowbar placed in the slot above the right door, you should report it to the telco *at once!* On the

inside of the door, there should be a circular attachment with a "D"-type test cord on it which makes accessing pairs with a test set easier (if you don't have a test set, I will describe how to make a basic one later in this article). You should hook the alligator clips on your test set to the two bolts on the attachment, and then use the specialized cord to hook up to binding posts on the panel (it is specially designed to do so, whereas alligator clips aren't). There are usually also spare decals and 2 reels of #22 solid "F" cross-connect wire stored somewhere in the cabinet, either on the doors in a box (along with a "788N1" tool for seating and trimming jumper wires) or mounted in the splice chamber (described in the next section).

Locating Pairs and Cross-Connects

Basically, the SAI cabinet contains several terminal block panels (size A=1 panel, size C+D (800+1200 pairs, respectively) =2 panels, size E=3 panels) of either 76-type screw binding posts (the most common) or more modern 108-type "quick-connect" connectors. These panels are divided up into six blocks of 100 cable pairs (2 screws = 1 binding post, per cable pair) each, with block 1-100 on the top and 501-600 on the bottom. In a 2-panel cabinet, the left panel typically contains the pairs from the F1 (feeder) cable, and the right panel contains the F2 distribution cable pairs. This is accomplished by either a harness or cable stub whose pairs are internally connected to the binding posts on a panel. The harness or stub is then spliced, usually with "710" splicing connector modules, to the respective F1 or F2 cable. In the case of the harness, this splice is located in the back of the cabinet,

DISTRIBUTION PLANT

in the splicing chamber, which can be accessed by rotating the notched circular latch on the top of the terminal block assembly and letting the panel fall forward. Often the splices are covered with plastic bags. Note the color code of the pairs; if you can locate the pair you want, this is an excellent location to covertly access it, because this area is rarely seen during normal use of the cabinet (it is usually only opened during a cable cutover or "throw", in which a whole section of feeder or distribution cable is replaced at one time). In the case of cable stub, the splicing is usually done underground at a closure, because the raw-ended cable extends 20 to 100 feet from the cabinet; in this case, there won't be a splicing chamber. This type is often used for aerial pole-mounted SAI's. Also note that in an F-size cabinet, you have to remove the whole back panel in order to access the splice chamber. Anyway, the pairs from the feeder panel are cross-connected with wire jumpers over to the binding posts on the distribution panel; in this way, the two cables are connected.

There are several ways to locate a pair in an SAI. First, and best, if you have

assignment data from LMOS or equivalent, there should be an F1 Binding Post (BP) number listed alongside the cable numbers. This number is usually a 3 digit number, 001-999, and it will correspond to a binding post pair in one of the hundred-blocks on the feeder panel side. The first digit of the BP is the block, and the other digits represent the pair in that block.

The color of the pair label is important, also -- feeder pairs are always marked with *green* labels. Secondly, if you don't have a binding post number, there may be a log or other chart posted on one of the doors of the cabinet showing the cable pairs and their corresponding binding posts (or the posts may in some cases be arranged or labelled in a way such that the cable pair number could be derived). Thirdly, as a last resort, you could connect a test set to each pair in the terminal, and dial your area's ANI number (This "ANI" number is usually a multi-digit test code which, when dialed, responds with a voice announcement of the Directory Number (DN) for the line you are dialing from). This would have to be repeated until you happen to hook up to the line you are looking for (it's time consuming, but it works).

				Terminal Panel	
		(Green)	(Blue)	F1 pairs	--F1----F2---
		-- F1 Feeder	----- F2 Dist.-----	==>001-100	! *** XXX !
F1 BINDING POST	!	XXXXXXXXXX	XXXXXXXXXX	!	! 101-200 ! XXX XXX !
# 025	!	XXXXXXXXXX SAI	XXXXXXXXXX	!	! 201-300 ! XXX XXX !
!	!	XXXXXXXXXX	XXXXXXXXXX	!	! 301-400 ! XXX XXX !
-----^				!	! 401-500 ! XXX XXX !
(^ close up view of first 3 of 10 binding post				!	! 501-600 ! XXX XXX !
rows of the first hundred block (marked ***))----				!	!-----!
F1 BP # 025 : 0 = first 100-block, 2 = pass over 2 full rows (go to 3rd row down), 5 = 5 pairs from left.					

OUTSIDE LOOP

Some sample ANI numbers are:

213 NPA - Dial 1223

213 NPA (GTE) - Dial 114

408 NPA - Dial 760

914 NPA - Dial 990

These numbers will vary from area to area, and some areas may not have such a service (in this case, you may have to dial a TSPS operator and have her read off the number on her ANI panel -- in some areas, you may have to say a code word or phrase in order for her to give you the number). In any case, it would be a good idea to ask a lineman or testboard employee for the procedure to use in your area to get ANI, because it's very useful and you'll need it sooner or later.

Anyway, once an F1 BP is found, the cross-connect wire can be traced over to the distribution panel, and in this way, the F2 pair can be found. These F2 distribution pairs are always marked with *blue* labels. Note also that the binding post number of the cross-connected F2 pair is not recorded in LMOS (the F2 BP is *not* in the SAI, so don't confuse an F2 BP number with a BP in the SAI); however, when the cables are first installed, the feeder pairs and distribution pairs are in sequence -- this makes it easy to visually assume where the F2 pair is. This order can be upset when cable pairs are added or changed, however, so it can't always be relied upon to produce valid F2 cable pair numbers (also, there may be two distribution cables, with the low-numbered pairs on the bottom and the high-numbered pairs on the top! It all depends on how the local telco sets things up).

Floaters / Multiples

All of the pairs in a feeder cable are

rarely used simultaneously; this would be impractical, because if one of the pairs was discovered to be faulty, or if a subscriber wanted another line, a whole new feeder cable would have to be added. To solve this, extra facilities are left in the loop plant as a provision for expansion. For example: on the feeder panel, all of the binding posts may be connected to F1 cable pairs, but not all of them may be crossed over to distribution pairs. These spare pairs are not connected to the switch, so they won't "have dial tone", but they are numbered. Since these lines aren't assigned, they won't be found in LMOS, but they will definitely be listed in LAC records. These records are the Dedicated Plant Assignment Cards (DPAC) / Line Cards and the Exchange Cable Conductor Records (ECCR), or even computerized databases (i.e., MODE). If the numbers can be found (or even noted, if the numbers on the binding posts at the SAI correspond with feeder cable pair numbers), then the lines can be activated via a COSMOS service order. This is aided even further by the fact that since F1's usually last longer than F2 facilities, there are often more spare provisional F2 facilities in the loop plant (i.e., 100 feeders in, 300 F2 out (200 aren't cross-connected to F1's)). So there is a good chance that you will find one that is distributed to your area. Other spare facilities include "floaters", which are like spare feeder pairs, except they are *active* lines. Often, a telco will extend whole feeder groups to more than one SAI in provision for future expansion, including active cable pairs. If you find a working pair on a feeder panel which is not cross-connected to a

DISTRIBUTION PLANT

distribution pair, that pair is a floater. This is by far the best way to covertly access a certain pair, because most linemen will probably not be aware of the pair's presence (it looks unused on the surface). Beware! If you think you can hook up to someone's floater and get free service, you're probably wrong (so many other people have been wrong, in fact, that Pacific Bell has a special "Form K-33" to report this type of fraud), because the telco is more aware of this than you may think. Obviously, any toll call you make will show up on the bill for that line. A do-it-yourself spare pair activation can avoid this problem, if done correctly.

Cable Facility F2 - Distribution

The F2 distribution cable is the cable which originates from the F1 feeder in the SAI and distributes individual cable pairs to each subscriber. This cable can be one of two types: aerial or buried. The most common is the aerial distribution cable, although buried cable is the modern trend. In the case of aerial F2, the cable or cables leave the SAI underground, and at the first telephone pole on the distribution span, the cable is routed up the pole. It then is suspended on the span, such as down a street, and at each group of houses there is a terminal on the span. This terminal is the aerial drop splitter, and its purpose is to break off several pairs from the distribution cable in order to distribute them (in the form of aerial drop wires) to each house or premise. The location or address of the premise nearest this aerial drop splitter is the Terminal Address of the F2 serving a certain pair (each group of pairs in the F2 will have its own terminal address, unlike the one address for the F1

terminal (SAI)). The F2 cable is always the lowest cable on the telephone pole, and it is usually a great deal larger than the electric power distribution cables above it. Often more than one F2 can be seen on a single pole span. In this case, the top F2 will usually be the one which is being distributed to the subscribers on that street, and the lower (and most often larger) cables are other F2's coming from an SAI and going to the streets which they service. These cables consist of multiple spliced spans, and they will not have any drop wires coming off them (they are marked every few poles or so at a splicing point called a "bullet closure" which is fully enclosed and can be quite large (i.e., 6" dia, 20" long) as compared to the normal drop splitters (i.e., or similar 4"w x 5"h x 12"l) -- these closures are clamp pressurized and are not meant to be opened unless the cable is being replaced or splicing work is being done. They are not standard cable/pair access points).

Buried F2 plant is similar to aerial, except that the cable is not visible because it is underground. Instead of going to a pole from the SAI, the cable continues underground. The drop wires are also underground, and the method of breaking them from the distribution cable is similar to that of the aerial drop splitter, except it is a small pedestal or box located on the ground near the houses it serves. This address closest to this pedestal is the TEA for the F2.

F2 Cable Numbering

The F2 distribution cable is usually given a 4 or 5 digit number, depending on the office. The first 2 or 3 digits should be the number of the F1 that the F2 was

OF PAIRS AND BOXES AND POLES

branched off of, and the last 2 or 3 digits identify the distribution cable. Example:

F1 Cable	F2 Cable
25	2531

This F2 cable came from feeder #25.

The cable *pair* numbers may be set in a similar way, with the last 3 or 4 digits identifying the pair, and the first digit (usually a one identifying the pair as a feeder or a distribution pair. Example:

F1 Cable	Pair	F2 Cable	Pair
25	1748	2531	748

^--signifies F1 (feeder) cable pair

Generally, the F1 cable pairs are numbered higher than the F2 cable pairs, due to the fact that a feeder cable may contain several distribution cables' worth of cable pairs. Note once again that all of this numbering plan is the *standard*, and it may be far from real life! As soon as one distribution pair is replaced, crossed over to another feeder pair, or taken from service, the set order is interrupted. In real life, it is most always necessary to get both F1 and F2 cable assignment data.

Facilities F3-F5,

Rural Area Interface (RAI)

Although cable facilities F3, F4, and F5 may be specified in any loop plant, they are rarely seen anywhere except in rural areas under the RAND plan (Rural Area Network Design). Basically, plants using these extra facilities are similar to F1/F2 plants, except there are extra cable spans and/or terminals in the path. When locating cables, the highest numbered facility will be at the end of the path, terminating near the subscriber's end (like a "normal"

F2), and the lowest numbered facility will be the feeder from the CO (like a "normal" F1). The extra spans will be somewhere in between, like an intermediate feeder or extra distribution cable with separate cable access terminals. One such facility is the Rural Area Interface (RAI), which can be used in a "feeder-in, feeder-out" arrangement. This is usually seen on cable routes of 50 pairs or greater, with a length of longer than 30 kft (about 6 miles). In this case, there will be two terminal cabinets in the feeder path, labelled RAI-A and RAI-B. The RAI-A is special because it has a two-part terminal block: the top has switching panels with 108-type connectors which cross-connect feeder-in and feeder-out pairs using jumper plugs, and the bottom has standard 76-type binding posts which cross-connect feeders to distribution cables for subscribers in the local area of the RAI-A. The jumper plugs can only be connected in one way to the switching panels, so random cross-connection of feeder-in/feeder-out pairs is prevented. In this way, the cable and pair numbers stay the same as if the feeder cable was uninterrupted. This is used a lot in rural areas; it allows part of a feeder group to be split off at the RAI-A like a distribution cable near a town along the route, and the rest of the feeder group continues on to a town further away, to the RAI-B where it is terminated as in a "normal" SAI. In order to access a pair, just use the last RAI in the span (whichever it is) and treat it just like an SAI. If the pair terminates at RAI-B, you can also access it at RAI-A! (If you can locate the pair using color code, BP number, or (ughh) ANI, there should be test terminals on top of the jumper plugs con-

(continued on page 34)

Federal Bureau of Investigation
Anti-Phone Sex Division

DEAR 26
You will SEND PILES
OF ALL Back ISSUES FROM 84
5 86 And 87 PLUS SEE ing 88 PLUS
A YEAR Subscription RENEW al THE
ADDRESS SHOWN ON THE en check
OR You WILL NEVER FIND
IT LERS' ER IN

Thank you,
Ed Reese

THIS IS WHAT WE HAVE TO PUT UP WITH.

OUTSIDE LOOP

(continued from page 32)

necting the 108's on the switching panel where you can hook your test set -- you can't hook onto a raw 108 connector very easily.) Anyway, the RAI terminal is usually a ground pedestal with a cabinet such as a 40-type, but it can be aerial mounted on a pole (hard to access).

Pair-Gain, Carried Derived Feeder

Another common facility in rural areas (and in cities or suburbs, especially near large housing complexes, etc.) is the pair-gain system. It is basically a system which consists of a digital link which is distributed, almost like a normal cable pair, out to a terminal cabinet called a Remote Terminal (RT) which contains equipment which demultiplexes the digital line into many "normal" metallic analog telephone lines which go to each subscriber in the area. Because the digital line can transmit the audio from several separate lines and multiplex them onto one cable, only one special cable pair is needed to come from the CO as a feeder, instead of several separate ones; this is why it is called a "pair gain" system. The remote terminal (RT) contains both the demultiplexing electronics as well as a small "SAI" type terminal block for connecting the pairs to distribution cables on the side of the path toward the subscriber. Because the "feeder" is not a multipair cable but a digital link (i.e., T-carrier), this arrangement is known as a "carrier-derived feeder". The SAI part of the RT is used just like a normal SAI on the distribution side (*blue*), but the feeder side will be slightly different. Carrier-derived feeders are always marked with *yellow* labels, and their pairs will be crossed over to distribution cables just like

in an SAI. So, in order to access a pair in a system like this, you must do so on the *distribution* side, because you can't hook an analog test set to a 1.544 Mbps digital T-carrier line! (or worse yet, a fiber optic cable). This may be difficult, because these cabinets are always locked (with few exceptions), so you'll have to find a terminal closer to the subscriber -- also be aware that many RT's are equipped with silent intrusion alarms. Anyway, some common pair-gain systems are the Western Electric SLC-8, 40, 96, and GTE's MXU, ranging in size from 8 to over 96 lines. RT cabinets can often be identified by the ventilation grilles (with or without a fan inside) which are not present on SAI's or other non-RT cabinets.

Aerial Distribution Splice Closure, Drop Wire Splitter

This terminal is the point where the individual cable pair for a certain subscriber is split from the F2 distribution cable and spliced onto an aerial drop or "messenger" wire which goes to the subscriber's premises. In an aerial distribution plant, two types of this terminal are common:

- 1) Western Electric 49-type Ready Access Closure / Cable Terminal
- 2) Western Electric 53A4, N-type Pole Mount Cable Terminals

Type 1: The 49-type, 1A1, 1B1, and 1C1 closures are all functionally similar. This terminal is a semi-rectangular closure, about 15"L x 3"W x 5"H, usually black, which is connected directly to the aerial cable itself; it is coaxial with the cable, so the cable passes straight through it. It splits up to 12 pairs from the distribution cable to a small binding post

DISTRIBUTION PLANT

terminal block inside the closure. Aerial drop wires are then connected to these binding posts, and the wires exit the terminal through holes on the bottom. These wires are strung via strain relief clamps on the pole down to the subscriber's site. The terminal closure is opened by pulling out and lifting either the whole cover or the front panel after removing the cover fasteners on the bottom and/or the sides (the closure is a thick neoprene cover over an aluminum frame). Inside the case, there is a terminal block and there may be some sort of loading coil as well. The cable and this coil are not openable, but the terminal block is. Since the F2 pair terminates in this closure, the F2 BP number (cable/assignment data) corresponds to a binding post on this terminal block. As mentioned earlier, this terminal will also contain spare pairs, in case a subscriber wants another line. In order to use one of these pairs, you must either get an F2 (and then F1) CP number from LAC using the BP, or you can put a trace tone on the pair at the aerial closure and then locate the pair at the SAI. Then a cross-connect would have to be made to an active F1 pair, and a drop wire (ughh) would have to be added back at the aerial closure. Anyway, both the binding posts as well as the holes (inside and out) are numbered left to right, so you may not even have to open the closure if you are just looking for an F2 BP number -- just trace the drop wire from the house into the numbered hole on the closure. The Terminal Address for the F2 is the address of the house or premise closest to the pole near this closure. These terminals (especially 1A1, etc.) are also used for straight and

branch splices for aerial cables, so you may see one cable in and two out; also, the closure can be used for splicing only, so there may not be drop wires (in this case, it won't be listed in LMOS because it is not a terminal point). There is generally one of these every pole near a quad of houses or so, mounted on the cable about an arm's length from the pole.

Type 2: Both the 53A4 and the N-type terminals serve the same function as the 49-type just described, except they are used in situations where there are more than 4 houses (8 lines, including provisional pairs). This terminal is mounted directly on the pole, about a foot down from the aerial cable. It is not connected in line with the cable, so there is no F2 splicing area in the cabinet (rather, a cable stub comes from the terminal block and is spliced onto the span close to where it touches the pole). It is about 22"H x 9"W x 4"D, rectangular, and silver (unpainted). The door is similar to that of a 40-type cabinet, but it's much smaller; it is opened using a 7/16" tool in the same manner as before, except that the door must be lifted before it can be opened or closed. In this way, the door slides down on its hinges when opened, so it locks in the open position and you won't have to worry about it (especially nice because hanging onto a pole is enough of a problem). The terminal block can handle from 25 to 50 pairs, with 32 holes in the back for aerial drop wires. Just as in the Ready Access Closure, this is the F2 terminal, and the numbered binding posts and holes correspond to F2 BP numbers. The TEA will be the address nearest the terminal (just as before). This terminal is common at the first pole on a

GETTING DIRTY,

street, on cul-de-sacs, apartments, marinas, and harbors, or anywhere there are many drop wires.

Buried Distribution Cross Box and Other Pedestals

This terminal serves the same function as the aerial closures, except it is used in areas with a buried distribution plant. This cable assignment for this terminal will be the F2 terminal, and the BP numbers and TEA will be the same as for the aerial terminals. Probably the most common cross boxes are the PC4, 6, and 12; these are around 50" tall by 4, 6, or 12" square respectively, and they are painted gray-green like SAI cabinets. These are the smallest pedestals in the distribution plant, and they don't have doors (they look like waist-high square poles). In order to open one of these pedestals, the two bolts on either side halfway down the pedestal must be loosened with a 7/16 hex wrench; then the front cover can be lifted up, out, and off the rest of the closure. These terminals are located generally near small groups of houses (up to about 12 lines usually) on the ground, often near other utility cabinets (such as electric power transformers, etc.). These are becoming more common as the new housing tracts use buried distribution plant. The F2 cable will enter as a cable stub, and it is split into service wires which go back underground to the subscribers.

All small pedestals are not necessarily the above type of terminal; these pedestal closures are often used for other purposes, such as splicing points in underground distribution, loading coil mounting, and even temporary wire storage containers. If the terminal contains a terminal block or it

is a significant point on the line, however, it will be listed in LMOS. An example of this is a distribution path found by Mark Tabas in a Mountain Bell area -- there was a small PC12-type closure on the ground near a street in a remote suburb, and it was serving as a terminal point for a whole F1 cable. It was listed as the F1 terminal, and it was at the right TEA; however, there was no terminal block because it was a splicing point (just a bunch of pairs connected with Scotchlok plastic connectors which are hung on a bar in the pedestal closure), so LMOS had no BP number. Instead, a color code was listed for the pair in the splice. Anyway, the *whole* F1 went up to an N-type closure on a pole and was split into drop wires.

Multi-Line Building Entrance Terminals

This terminal takes the aerial drop or service wires and cross-connects them over to the Inside Wire (IW) in the subscriber's building (hotels, businesses, etc.). There are many different types of terminal blocks for this terminal, although by far the most common is the Western Electric 66 block. The 66-type terminal uses a block of metal clips; the wire is pushed onto the clip with a punch-down tool which also strips the wire. The block is divided into horizontal rows which can have from two to over six clips each. Since each row group terminates one pair, two rows are needed for x-connect, one on top of the other. The service or drop wire usually enters on the left, and the inside wire is connected to the far right. In order to locate a pair, usually you can visually trace either the service wire or the inside wire to the block, and often the inside wire side will be numbered or labelled with an

BEING SNEAKY

address, phone number, etc. It is also possible for this terminal to serve as an F2 terminal point, if there are a lot of lines. In this case, LMOS will list the TEA usually with some physical direction as to where to find it. The left side will then be numbered as F2 BP's. This terminal is also the demarcation point which separates the customer's equipment from the telco's. The new terminals often have an RJ-21 connector on the service wire side, such as a 25-pair for PABX or a Bell 1A2 Key, etc. There are also "maintenance terminating units" (MTU) which are electronic units connected to the line(s) at the entrance protector; these are sometimes seen in some telcos. Basically, they provide functions such as party ANI on multi-party lines, remote disconnect (for testing or (click!) non-payment), or half ringers (the most common -- they prevent ringing continuity failures on switches like ESS when there are no phones hooked to the line when it rings). MTU terminals are often locked.

Single Pair Station Protector

There's really not much to say about this terminal. Basically, it takes the service

or drop wire and connects it to the inside wire in a single line residence (houses with two lines will have two of these). These are at every house on an outside wall or basement, and there are two main types: the Western Electric 123 (with a "150-type" rubber cover), and the old WE 305 and new AT&T 200 Network interface (metal and plastic, respectively). These terminals have one binding post pair and they will have either gas discharge tubes or carbon blocks to protect the line from lightning or excess current. Obviously, there is no BP number (you just have to visually trace the drop wire to find the protector). This is also the demarcation point marking the end of the telco's responsibility, as well as the end of our tour.

Usually if a color code is needed (such as in a splice case) you can get it from LAC or the testboard; if it's really essential, it will be in LMOS as well. This color code is also used a lot on cable ties (usually with white stripes and ring colors only), although these are often used randomly.

Test Sets

This is the "right hand" of both the pro-

Bell System Standard Color Code

Pair #	Tip	Ring
01-05	White	Blue
06-10	Red	Orange
11-15	Black	Green
16-20	Yellow	Brown
21-25	Violet	Slate

Use:

Take the #, and find its closest multiple of 5. Use that number to find the Tip color, and the remainder to find the Ring color (remainder 0 = Slate). (e.g. Pair #1 = White/Brown, Pair #14 = Black/Brown, Pair #24 = Violet/Brown).

OUTSIDE LOOP DISTRIBUTION PLANT

OFFICIAL Agent 04 Generic Test Set Modification (tm)

```
Ring >-----> to "test set" phone
Tip >-----! SPST Switch !----->
          !-----/-----!
>from          !-----/!/!/!/!----! C = 0.22 uF 200 WVDC Mylar
cable pair     ! C      R      !      R = 10 kOhm 1/2 W
(alligators)  !--! (-----! SPST = talk / monitor
```

fessional and the amateur lineman. Basically, it is a customized portable telephone which is designed to be hooked onto raw cable terminals in the field and used to monitor the line, talk, or dial out. The monitor function is usually the main difference between the "butt-in" test set and the normal phone. If you don't have a real test set already, the following circuit can convert a normal \$4 made-in-Taiwan phone into a working test set. The "all-in-one" handset units without bases are the best (I tend to like QUIK's and GTE Flip Phone II's).

When SPST is closed, you are in talk mode; when you lift the switchhook on the "test set" phone, you will get a dial tone as if you were a standard extension of the line you are on. You will be able to dial out and receive calls. When the SPST is opened, the resistor and capacitor are no longer shunted, and they become part of the telephone circuit. When you lift the switchhook on the test set, you will not receive dial tone, due to the fact that the cap blocks DC, and the resistor passes less than 4 mA nominally (far below the amount necessary to saturate the supervisory ferrod on ESS or close the line relay on any other switch). However, you will be able to silently monitor all audio on the

line. The cap reactance plus the phone's impedance ensure that you won't cut the signal too much on the phone line, which might cause a noticeable change (expedite the shock force, *someone's on my line!!*). It's also good to have a VOM handy when working outside to rapidly check for active lines or supervision states. Also, you can buy test equipment from these companies:

Techni Tool, 5 Apollo Road, Box 368, Plymouth Meeting, PA 19462.

Specialized Products Company, 2117 W. Walnut Hill Lane, Irving, TX 75229.

I am not going to include a disclaimer, because a true communications hobbyist does not abuse nor does he tamper with something he doesn't understand. This article is intended as a reference guide for responsible people.

Also, this article was written mainly from first-hand experience and information gained from maintenance technicians, test boards, as well as technical literature, so it is as accurate as possible. Keep in mind that it is mainly centered upon the area served by Pacific Telephone, so there may be some differences in the loop plant of your area.



Illinois Bell
AN AMERITECH COMPANY

Dear Employee

We are in the process of launching a major market thrust to stimulate usage revenue in the 4th Quarter 1987. As part of this undertaking we are pleased to announce a first time marketing promotion.

Through special arrangements with Graybar Electric Co. Inc., we are able to offer a select group of customers the opportunity to purchase state-of-the-art telephone answering machines at steep discounts. We have chosen to promote answering machines because they increase call completions which result in usage revenue.

This offer is being made to a select target market in order to maximize sales success. The success of this experimental offer will determine our future efforts with promotions of this type.

Because this first-time arrangement includes a savings of 40% to 46% on telephone answering machines, we want to offer this opportunity to all our employees. You too have the option of selecting from three deluxe models at great prices and to enjoy the ease and convenience of owning a telephone answering machine.

See the enclosed brochure for details. This offer is good until December 31, 1987, so be sure to act soon.

Sincerely,

Rita Zaccardelli
Product Management

P.S.....remember, answering machines also make very nice gifts.

HERE WE SEE what the phone companies are really interested in: call completions. Does this surprise you?

2600 Marketplace

FOR SALE: Various UNIX manuals/books. For more information, write to Seth K., PO Box 245070, Brooklyn, NY 11224.

I WANT TO START a newsletter devoted to petty crimes, tentatively titled "For Informational Purposes Only". Please send me info, clippings, on how to rip-off vending machines, free postage, free photocopies, sneaking into movie theaters, etc. Tim Cridland, PO Box 85874, Seattle, WA 98145.

WANTED: Someone with electronic ability to build a red box similar to the plans in Sum-

mer 2600 or a blue box at a reasonable cost for test purposes. Write to: Nelson, 302 North 15th, Richmond, IN 47374.

WILL TRADE: My Texas Instrument Silent 700 Series Portable Intelligent Data Terminal (like new) w/full documentation for any hacker software for IBM compatible computers. Ted K., PO Box 533, Auburn, NY 13021-0533.

COMPLETE RANGE of Commodore 64 hack/phreak software. All tested and debugged. Many advanced applications. Call THC-[] BBS at 604-595-0085 and leave feedback to the sysop for more information.

WANTED copied (dead) or alive! TAP'S "C" & "D" elec. courses. Cassette tape (TAP exclusive), & fact sheets #1-4. Have any or all? Contact me--willing to pay good money for orig's. B. Barton, 84 Daphne Cres., Barrie, Ontario L4M 2Y9. (705-726-6617)

WANTED: All newer hardware you

find a must to quickly get rid of. Product evaluations are welcomed. Also looking for Technics SL1200 and any information related to pirate radio (including stories written by ex-pirates, groups, equipment information, FCC) for a write-up. David Jon Hyams, E 9116 Sprague Av., Apt. 111, Spokane, WA 99206

SELLING COPIES of Abbie Hoffman's "Steal This Book". \$7.95 + \$2 shipping & handling. Marco, P.O. Box 1211, Westerly, RI 02891.

FOR SALE: Ultimate blue box, Berry Electronics Model 312A trunk test set,

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.

has rotary dial/MF keypad, monitor speaker. Uses L-C oscillators. VERY stable. Can be used as Std phone when head/handset added.

\$250. Write: Testset, 6715 Eberlein Ave., Klamath Falls, OR 97603.

TAP BACK ISSUES, complete set Vol. 1-90 of QUALITY copies from originals. Includes schematics and indexes. \$100 postpaid via UPS or First Class Mail. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info.

Deadline for Winter Marketplace: 11/30/88.

Happenings in Our World

(continued from page 13)

owner can then call the machine and give it commands.

Again, there's a big problem here. All someone has to do is call and hang up, this time only once. If nobody picks up the phone at the other number, call forwarding is cancelled, which may not be desired.

Both of these inventions are good ideas. But without decent security, they could be real disasters for the consumer. Imagine having all of your calls forwarded to some remote place where a tape recording could give out false information about you or your business. And the real clincher is the fact that you'd have to *pay* for those calls!

Sysop Sued Over Email

An Indiana BBS operator is being sued by a user who claims that he intentionally disclosed her private electronic mail to others without her permission.

The lawsuit makes reference to the Electronic Communications Privacy Act of 1986, which makes disclosure of private electronic mail without consent of the sender or the recipient a federal crime.

Sysops are not by law required to offer private electronic mail to its users. But in cases where they do, the ECPA can be used against them if they don't keep private mail private.

This is what we've been wait-

ing for. Finally, ordinary BBS users are getting something out of the ECPA, which never really seemed designed to protect the individual.

This is a first step towards assuring privacy from the snooping eyes of authority. It won't be so easy to expect a system operator to know every message on his/her system, much less assume responsibility for them.

Our own bulletin boards, as always, will provide private mail features for users. We don't read or disclose private messages; in fact, our software won't even permit it. We hope this lawsuit will encourage other sysops to adopt this practice and discourage law enforcement from violating our right to privacy.

Dial-It Info Numbers

At long last, New York Telephone has come out with a guide to all of those new mass announcement numbers.

Dialing 540-INFO (toll-free) will get you a list of all 540 interactive services, as well as all of the 976 passive announcement numbers. Dialing 970-INFO gets you a list of all of the adult services (really funny to hear) and 550-INFO will generate a list of the conference numbers. To get a physical list, dial 800-942-1818, operator 976.

If anyone gets this to work outside of New York, let us know.

LETTERS

(continued from page 27)

Too bad, you lose. I am a telecom tech at a large centrex customer of Pac Bell (actually, a management position). We are such a good customer that I can call the CO and get them to do anything. They do it because we are such a good customer. Not because I lie and tell stories like some do.

I had hoped to share some of this information and my 40+ years of experience with others, but I am not going to waste my time to learn your BBS.

I was a writer for TAP and know the whole story of what happened. Would like to share this also -- but your damn BBS pisses me off!

I also have a patent in telephony and a manufacturing company that makes telephone stuff under the patent.

Whenever you get a normal BBS, let me know and maybe I will change my mind.

Boy, it sure feels good to write this letter.

Am in San Francisco today to tour Pacific Bell's San Ramon complex. I am their guest. They pick me up at my hotel and give me lunch and a tour. This is because I am a good customer of theirs and I am designing the telecommunications facilities for a \$44 million building going up in the

next two years.

See what you missed!

Boy, it even feels better now.

Change those BBS's!

Sorry I can't leave you my name. I am somewhat well known in the field and information I provide must not have my name on it.

We enjoyed your letter very much. We can certainly see how you managed to become so well known. And, no doubt, using your name would not be a good idea, in this or any circumstance. But we do want to thank you for finding time in your busy schedule to convey your concerns.

Unfortunately, no one here has any idea on what you could be talking about. We operate four BBS's, each running on completely different software. You seem to have had a run-in with one of them. Why don't you tell us exactly what happened so we can do something about it?

Questions

Dear 2600:

For starters I would like to say that this is the best magazine I ever laid hands on. I like the professional way you look at everything. In your November 87 issue the ad that Consumertronics put in was great for me because I found a file on getting me some fake

LETTERS

ID's. It says that having them is not illegal. Can you tell me where this came from? Everyone I spoke to says it is a lie and just there to get you to buy the product. Can you tell me if there are any voice systems to play around with? There was one in Philly called The Philly Connection. Are there any more out there? If so, can you list the numbers?

J.D.

The people who advertise in 2600 speak for themselves and not us. Therefore, you'll have to ask them what they mean. Our policy is to accept advertising from anyone unless it makes us violently ill or we know that the people are crooks.

We will be printing phone lists of all kinds of systems as we get them in.

Another Scam

Dear 2600:

I am writing you to pass along some information, and to ask the readers of 2600 about any experiences they may have had with a company called "Mutual Telecommunications Network, Inc.". My first experience with them was in November 1987. They put an ad in my local paper for "computer syop". The basic idea was as follows: They send you "\$1,200.00" worth of circuit boards, modems, software, etc.

You install it, and let them use your phone from 9 am to 9 pm, 7 days a week. After 9 pm, you prepare the data obtained that day for transmission to the company's computer(s). The company in turn pays you an hourly rate of \$3.57 per hour, per day that your system (IBM PC compatible only) is up and running, up to a maximum of \$300.00 per week.

I filled out the application and the agreement, including, stupidly enough, the personal financial information. I also indicated on the application that I did not want to pay the \$660.00 security deposit. I sent the letter back to the Florida address on the envelope, and got back a response from a Los Angeles address. They rejected me, "having found others more qualified". I am a system administrator for UNIX and MS-DOS systems, and have been involved with computers for over five years. The only thing I could think of that would disqualify me was my unwillingness to shell out \$660.00 in a hurry just to sign up for this "hot deal".

In January 1988, the company mailed me another letter, offering me an opportunity to join again, but based on the dates in the letter, I had less than 7 days to send in my

LETTERS

\$660.00 security deposit. All my efforts to contact the company were for naught. I kept getting into some kind of digitized voice control system that threatened to have my phone number traced and reported to the authorities. I also tried the Better Business Bureau, the Chamber of Commerce, and all the phone numbers each one referred me to, but I was not able to contact anyone or anything, much less find out about the company. Even directory assistance gave me a phone number that fed into this control system. Unless you have the proper codes, you cannot contact any human employees in this company. I am concerned that this company is either attempting to collect personal information for the wrong reasons, i.e., credit card fraud, or they are a scam operation that makes its money by selling telephone networking equipment to home computer owners interested in extra income.

The phone numbers I have for this company are: (800) 553-8003 and (813) 932-1023. Their address is 7933 North Armenia Avenue, Tampa, Florida 33604. I don't have the address or phone number any longer for the Los Angeles office. I also wrote to the Los Angeles Better Business

Bureau about these people, as well as a complaint letter to the company itself, all to no avail. The letter from the company ignored my questions and concerns, and I've never heard from the LA BBB. Please publish this letter in your magazine, so other people can either help find out if it's a legitimate operation or not. Needless to say, I never sent in any money, nor will I be doing business with them in the future. You may publish my name and address in your magazine, if you wish.

**Doug Porter
(FDP Enterprises)
3661 N. Campbell Ave.
#342
Tucson, AZ 85719**

Your letter was sent to us in January and we regret having waited so long to print it. The numbers you gave us have been disconnected. So, for one reason or another, this company is not thriving, at least not publicly. We call on our readers to watch out for this kind of thing and to let us know if they hear of anything similar. Thanks for passing this along.

Anti-Gay Offensive

Dear 2600:

Your nodding attention to the gay conference line com-

LETTERS

ment "(kill 'em!!)" in 2600, Volume 5, Number 2 is hardly appropriate. Most publications reserve the right to edit or to refuse to print material as objectionable as that. So I can't take your vaguely moral, "face-the-fact" disclaimer very seriously. Do you really think you've done anybody a service by reprinting that item, with or without a disclaimer?

I think you owe apologies not only to the gay community, but also to users of computers, telephones, and 800 numbers everywhere.

**CH
Ohio**

We do not believe in cover-ups. By not printing that bit of ugliness, we would have been

doing just that. The fact of the matter is, that comment was already on BBS's all over the country. Perhaps you misunderstood. We did not comprise that list ourselves -- it was taken off of a board.

If a public figure made a racist remark, would you blame the local newspaper for printing it? Would you expect them to pretend it didn't happen? Racism and its assorted relatives thrive when people try to deny their existence. Computer hackers are not immune from any of this. We can only hope that they, along with most of the others in the world, will look for injustice and scream about it when they find it.

„Hacker“ frei

Das Vorstandsmitglied des Hamburger Chaos-Computer-Clubs, Steffen Wernery, ist aus der Untersuchungshaft in Paris entlassen worden. Gestern traf der 26-jährige auf dem Flughafen Hamburg-Fuhlsbüttel ein. Das Verfahren gegen ihn wurde jedoch nicht eingestellt, sagte Wernery. Nach einem Haftprüfungstermin sei lediglich die Inhaftierung aufgehoben worden. Für weitere Vernehmungen müsse er wieder nach Paris zurück.



2600 T-SHIRTS

No, we're not kidding. On the front, you'll find an impressive masthead, with the 2600 title visible for very long distances. And on the back, you'll be displaying a collection of news clippings about phreaking and hacking from newspapers all over the world! A great conversation starter on supermarket check-out lines!

Let the world know how enlightened you really are.

\$10 per shirt.

Sizes available: S, M, L, XL.

No returns regardless of what you say or do.

Allow 4 to 6 weeks for delivery.

(Clip here and send in -- your address is on back.)

Send all orders to:

2600

PO Box 752

Middle Island, NY 11953 U.S.A.

(516) 751-2600

Subscription renewals: \$15 ind./\$40 corp.

Back issues: \$25 per year starting in 1984.

TELL US WHAT YOU WANT:

CONTENTS

OUTSIDE LOOP INFO	4
CELLULAR PHONES	8
WHO WAS STROWGER?	9
COMMUNICATIONS UPDATE	10
A MAP OF THE 516 NPA	14
RED BOX PROGRAM	22
CANADIAN NUMBERS	23
LETTERS	24
2600 MARKETPLACE	41

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

SECOND CLASS POSTAGE

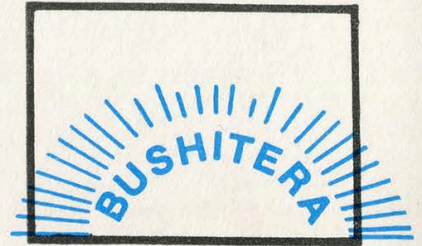
Permit Pending at
East Setauket, N.Y.
11733

ISSN 0749-3851

DANGER:
MISSING LABEL

2600

The Hacker Quarterly



Volume 5, Number 4

Winter, 1988-89



1884 saw the beginning of public call offices.
The National Telephone Company charged 2d
(or 1p) for a three minute call.

The National Telephone Company, Limited.

PUBLIC CALL OFFICE.

TARIFF.

LOCAL CALLS (Metropolitan Exchange Area).

For every 3 minutes conversation, or part thereof (whether originated or received), a fee of

2^{D.}

for the use of the Call Office.

INSTRUCTIONS.

TO CALL THE EXCHANGE.—Turn the handle, place the receiver to the ear, tell operator the Exchange and number of the subscriber required, then wait with the receiver to the ear, unless the operator says she will ring you.

When requested by the operator, but not before, place two pennies in the slot and press the button after the insertion of each penny, still keeping the receiver to your ear. The operator has the means of checking the amount. Bent or misshaped Pennies must not be used.

If more than 3 minutes conversation is required the extra money must be put in at the request of the operator. Callers are only allowed 6 minutes continuous conversation.

When your conversation is finished, replace the telephone on its rest and turn the handle.

NOTES.

Unless the telephone is on its rest you cannot call or be called.

Unless the key in the handle of the telephone is kept depressed you cannot be heard by your correspondent.

When two Subscribers are connected, and one of them leaves the instrument, his telephone should be replaced on its rest, the other Subscriber keeping the receiver to his ear and replying promptly should the operator ask if he has finished.

The handle should never be turned except to call the Exchange or to get disconnected.

If Subscriber required is engaged, ask again after a short interval.

The metal passes which were some time ago issued to London Subscribers, are obsolete. Persons producing these passes will be charged the same rate as charged to a Non-subscriber.

The Clerk-in-charge of the Exchange will reply to enquiries. Operators are forbidden to converse with Subscribers.

The public are notified that their strict adherence to the above rules is absolutely essential, and that only by this can efficient working of the system be attained.

Wm. E. L. GAINE,
GENERAL MANAGER

We Know

You should have had this issue last month. We know. We're sorry.

But just because we avoided the holiday rush (by not contributing to it) doesn't mean that you'll be losing out. In fact, we used the extra time to further pursue the late breaking MCI scandal (see page 10) as well as a couple of other stories, including the latest on the famous virus.

We've been playing with our new adjunct frame (mentioned last time

in this column) and are rather pleased with the results. We have all of the advantages of equal access and direct overseas dialing without having an electronic or digital switch. The extra time involved to complete a call is negligible. And touch tones are still free!

The MCI story is the first result of our new toy. As we scan out different companies and investigate them, more tales will unfold.

STAFFBOX

Editor-In-Chief

Emmanuel Goldstein

Office Manager

Bobby Arwatt

Artwork

Tish Valter Koch

Writers: Eric Corley, Thomas Covenant, John Drake, Mr. French, The Glitch, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOC, David Ruderman, Lou Scannon, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1988, 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada -- \$15 individual, \$40 corporate.

Overseas -- \$25 individual, \$55 corporate.

Back issues available for 1984, 1985, 1986, 1987 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.

2600 Office Line: 516-751-2600

BBS #1 (OSUNY): 914-725-4060 (down at the moment)

BBS #2 (CENTRAL OFFICE): 914-234-3260

BBS #3 (YOYODYNE): 402-564-4518

BBS #4 (BEEHIVE): 703-823-6591

BBS #5 (HACKER'S DEN): 718-358-9209

USENET ADDRESS: 2600@dasys1.UUCP

ARPANET ADDRESS: phri!dasys1!2600@nyu

A Report on the

by Bob Page

University of Lowell

Computer Science Department

(Reprinted from the RISKS Newsletter, an electronic publication available on many machines that are accessible by networks.)

Here's the scoop on the "Internet Worm". Actually it's not a virus -- a virus is a piece of code that adds itself to other programs, including operating systems. It cannot run independently, but rather requires that its "host" program be run to activate it. As such, it has a clear analogy to biological viruses -- those viruses are not considered live, but they invade host cells and take them over, making them produce new viruses.

A worm is a program that can run by itself and can propagate a fully working version of itself to other machines. As such, what was set loose on the Internet was clearly a worm.

This data was collected through an emergency mailing list set up by Gene Spafford at Purdue University, for administrators of major Internet sites -- some of the text is included verbatim from that list.

The basic object of the worm is to get a shell on another machine so it can reproduce further. There are three ways it attacks: sendmail, fingerd, and rsh/rexec.

The Sendmail Attack

In the sendmail attack, the

worm opens a TCP connection to another machine's sendmail (the SMTP port), invokes debug mode, and sends a RCPT TO that requests its data be piped through a shell. That data, a shell script (first-stage bootstrap) creates a temporary second-stage bootstrap file called x\$\$,l1.c (where "\$\$" is the current process ID). This is a small (40-line) C program.

The first-stage bootstrap compiles this program with the local cc and executes it with arguments giving the Internet hostid/socket/password of where it just came from. The second-stage bootstrap (the compiled C program) sucks over two object files, x\$\$,vax.o and x\$\$,sun3.o from the attacking host. It has an array for 20 file names (presumably for 20 different machines), but only two (vax and sun) were compiled in to this code. It then figures out whether it's running under BSD or SunOS and links the appropriate file against the C library to produce an executable program called /usr/tmp/sh -- so it looks like the Bourne shell to anyone who looked there.

The Fingerd Attack

In the fingerd attack, it tries to infiltrate systems via a bug in fingerd, the finger daemon. Apparently this is where most of its success was (not in sendmail, as was originally reported). When fingerd is connected to, it reads its arguments from a pipe, but doesn't

Internet Worm

limit how much it reads. If it reads more than the internal 512-byte buffer allowed, it writes past the end of its stack. After the stack is a command to be executed ("/usr/ucb/finger") that actually does the work. On a VAX, the worm knew how much further from the stack it had to clobber to get to this command, which it replaced with the command "/bin/sh" (the bourne shell). So instead of the finger command being executed, a shell was started with no arguments. Since this is run in the context of the finger daemon, stdin and stdout are connected to the network socket, and all the files were sucked over just like the shell that sendmail provided.

The RSH/REXEC Attack

The third way it tried to get into systems was via the .rhosts and /etc/hosts.equiv files to determine "trusted" hosts where it might be able to migrate to. To use the .rhosts feature, it needed to actually get into people's accounts -- since the worm was not running as root (it was running as daemon) it had to figure out people's passwords. To do this, it went through the /etc/passwd file, trying to guess passwords. It tried combinations of: the username, the last, first, last and first, nicknames (from the GECOS field), and a list of

special "popular" passwords:

aaa, academia, aerobics, airplane, albany, albatross, albert, alex, alexander, algebra, aliases, alphabet, ama, amorphous, analog, anchor, andromache, animals, answer, anthropogenic, anvils, anything, aria, ariadne, arrow, arthur, athena, atmosphere, aztecs, azure.

"It is pretty successful in finding passwords, as most people don't choose them very well."

bacchus, bailey, banana, bananas, bandit, banks, barber, baritone, bass, bassoon, batman, beater, beauty,

beethoven, beloved, benz, beowulf, berkeley, berliner, beryl, beverly, bicameral, bob, brenda, brian, bridget, broadway, bumbling, burgess.

campanile, cantor, cardinal, carmen, carolina, caroline, cascades, castle, cat, cayuga, celtics, cerulean, change, charles, charming, charon, chester, cigar, classic, clusters, coffee, coke, collins, comrades, computer, condo, cookie, cooper, cornelius, couscous, creation, creosote, cretin.

daemon, dancer, daniel, danny, dave, december, defoe, deluge, desperate, develop, dieter, digital, discovery, disney, dog, drought, duncan.

eager, easier, edges, edinburgh, edwin, edwina, egghead, eiderdown, eileen, einstein, elephant, elizabeth, ellen, emerald, engine, engineer, enterprise,

The Virus

enzyme, ersatz, establish, estate, euclid, evelyn, extension.

fairway, felicia, fender, fermat, fidelity, finite, fishers, flakes, float, flower, flowers, foolproof, football, foresight, format, forsythe, fourier, fred, friend, frighten, fun, fungible.

gabriel, gardner, garfield, gauss, george, gertrude, ginger, glacier, gnu, golfer, gorgeous, gorges, gosling, gouge, graham, gryphon, guest, guitar, gumption, guntis.

hacker, hamlet, handily, happening, harmony, harold, harvey, hebrides, heinlein, hello, help, herbert, hiawatha, hibernia, honey, horse, horus, hutchins.

imbroglio, imperial, include, ingres, inna, innocuous, irishman, isis.

japan, jessica, jester, jixian, johnny, joseph, joshua, judith, juggle, julia.

kathleen, kermit, kernel, kirkland, knight.

ladle, lambda, lamination, larkin, larry, lazarus, lebesgue, lee, leland, leroy, lewis, light, lisa, louis, lynne.

macintosh, mack, maggot, magic, malcolm, mark, markus, marty, marvin, master, maurice, mellon, merlin, mets, michael, michelle, mike, minimum, minsky, moguls, moose, morley, mozart.

nancy, napoleon, nepenthe, ness, network, newton, next, noxious, nutrition, nyquist.

oceanography, ocelot, olivetti, olivia, oracle, orca, orwell, osiris,

outlaw, oxford.

pacific, painless, pakistan, pam, papers, password, patricia, penguin, peoria, percolate, persimmon, persona, pete, peter, philip, phoenix, pierre, pizza, plover, plymouth, polynomial, pondering, pork, poster, praise, precious, prelude, prince, princeton, protect, protozoa, pumpkin, puneet, puppet.

rabbit, rachmaninoff, rainbow, raindrop, raleigh, random, rascal, really, rebecca, remote, rick, ripple, robotics, rochester, rolex, romano, ronald, rosebud, rosemary, roses, ruben, rules, ruth.

sal, saxon, scamper, scheme, scott, scotty, secret, sensor, serenity, sharks, sharon, sheffield, sheldon, shiva, shivers, shuttle, signature, simon, simple, singer, single, smile, smiles, smooch, smother, snatch, snoopy, soap, socrates, sossina, sparrows, spit, spring, springer, squires, strangle, stratford, stuttgart, subway, success, summer, super, superstage, support, supported, surfer, suzanne, swearer, symmetry.

tangerine, tape, target, tarragon, taylor, telephone, temptation, thailand, tiger, toggle, tomato, topography, tortoise, toyota, trails, trivial, trombone, tubas, tuttle.

umesh, unhappy, unicorn, unknown, urchin, utility.

vasant, vertigo, vicky, village, virginia.

We Were All Waiting For

warren, water, weenie, what-not, whiting, whitney, will, william, williamsburg, willie, winston, wisconsin, wizard, wombat, woodwind, wormwood.

yaco, yang, yellowstone, yosemite.

zap, zimmerman.

[I wouldn't have picked some of these as "popular" passwords, but then again, I'm not a worm writer. What do I know?]

When everything else fails, it opens `/usr/dict/words` and tries every word in the dictionary. It is pretty successful in finding passwords, as most people don't choose them very well. Once it gets into someone's account, it looks for a `.rhosts` file and does an "rsh" and/or "rexec" to another host, sucks over the necessary files into `/usr/tmp` and runs `/usr/tmp/sh` to start all over again.

Between these three methods of attack (sendmail, fingerd, `.rhosts`), it was able to spread very quickly.

The Worm Itself

The "sh" program is the actual worm. When it starts up it clobbers its argv array so a "ps" will not show its name. It opens all its necessary files, then unlinks (deletes) them so they can't be found (since it has them open, however, it can still access the contents). It then tries to infect as many other hosts as possible -- when it successfully connects to one host, it forks a child to continue the infection while

the parent keeps on trying new hosts.

One of the things it does before it attacks a host is connect to the telnet port and immediately close it. Thus, "telnetd: tloop: peer died" in `/usr/adm/messages` means the worm attempted an attack.

The worm's role in life is to reproduce -- nothing more. To do that it needs to find other hosts. It does a "netstat -r -n" to find local routes to other hosts & networks, looks in `/etc/hosts`, and uses the yellow pages distributed hosts file if it's available. Any time it finds a host, it tries to infect it through one of the three above methods. Once it finds a local network (like 129.63.nn.nn for ulowell) it sequentially tries every address in that range.

If the system crashes or is rebooted, most system boot procedures clear `/tmp` and `/usr/tmp` as a matter of course, erasing any evidence. However, sendmail log files show mail coming in from user `/dev/null` for user `/bin/sed`, which is a tipoff that the worm entered.

Each time the worm is started, there is a 1/15 chance (it calls `random()`) that it sends a single byte to `ernie.berkeley.edu` on some magic port, apparently to act as some kind of monitoring mechanism.

The Crackdown

Three main 'swat' teams from Berkeley, MIT, and Purdue found copies of the VAX code (the `.o`

Chaos in the

files had all the symbols intact with somewhat meaningful names) and disassembled it into about 3000 lines of C. The BSD development team poked fun at the code, even going so far to point out bugs in the code and supplying source patches for it! They have not released the actual source code, however, and refuse to do so. That could change -- there are a number of people who want to see the code.

Portions of the code appear incomplete, as if the program development was not yet finished. For example, it knows the offset needed to break the BSD fingerd, but doesn't know the correct offset for Sun's fingerd (which causes it to dump core); it also doesn't erase its tracks as cleverly as it might; and so on.

The worm uses a variable called "pleasequit" but doesn't correctly initialize it, so some folks added a module called `_worm.o` to the C library, which is produced from: `int pleasequit = -1;` the fact that this value is set to -1 will cause it to exit after one iteration.

The close scrutiny of the code also turned up comments on the programmer's style. Verbatim from someone at MIT: "From disassembling the code, it looks like the programmer is really anally retentive about checking return codes, and, in addition, prefers to use array indexing instead of pointers to walk through arrays."

Anyone who looks at the binary will not see any embedded strings -- they are XOR'ed with 81 (hex). That's how the shell commands are imbedded. The "obvious" passwords are stored with their high bit set.

Although it spreads very fast, it is somewhat slowed down by the fact that it drives the load average up on the machine -- this is due to all the encryptions going on, and the large number of incoming worms from other machines.

[Initially, the fastest defense against the worm is to create a directory called `/usr/tmp/sh`. The script that creates `/usr/tmp/sh` from one of the `.o` files checks to see if `/usr/tmp/sh` exists, but not to see if it's a directory. This fix is known as "the condom".]

Now What?

None of the ULowell machines were hit by the worm. When BBN staffers found their systems infected, they cut themselves off from all other hosts. Since our connection to the Internet is through BBN, we were cut off as well. Before we were cut off, I received mail about the sendmail problem and installed a patch to disable the feature the worm uses to get in through sendmail. I had made local modifications to fingerd which changed the offsets, so any attempt to scribble over the stack would probably have ended up in a core dump.

Most Internet systems running 4.3BSD or SunOS have installed

Computer Networks

the necessary patches to close the holes and have rejoined the Internet. As you would expect, there is a renewed interest in system/network security, finding and plugging holes, and speculation over what will happen to the worm's creator.

If you haven't read or watched the news, various log files have named the responsible person as Robert Morris Jr., a 23-year old doctoral student at Cornell. His father is head of the National Computer Security Center, the NSA's public effort in computer security, and has lectured widely on security aspects of UNIX.

Associates of the student claim the worm was a "mistake" -- that he intended to unleash it but it was not supposed to move so quickly or spread so much. His goal (from what I understand) was to have a program "live" within the Internet. If the reports that he intended it to spread slowly are true, then it's

possible that the bytes sent to ernie.berkeley.edu were intended to monitor the spread of the worm. Some news reports mentioned that he panicked when, via some "monitoring mechanism" he saw how fast it had propagated.

A source inside DEC reports that although the worm didn't make much progress there, it was sighted on several machines that wouldn't be on its normal propagation path, i.e. not gateways and not on the same subnet. These machines are not reachable from the outside. Morris was a summer intern at DEC in '87. He might have included names or addresses he remembered as targets for infesting hidden internal networks. Most of the DEC machines in question belong to the group he worked in.

The final word has not been written -- I don't think the FBI has even met with this guy yet. It will be interesting to see what happens.

DO YOU HAVE A FULL SET OF 2600 BACK ISSUES?

They're available at a rate of \$25 per year ordered. Back issues start with 1984 and include every issue up to the present.

(1988 issues are still available at \$5 each. All others are sold ONLY by year.) Send your order to:

2600 Back Issues

PO Box 752

Middle Island, NY 11953

MCI: The Phone Company With

It all started with what sounded like a friendly phone call in October:

"Hello, this is Patricia from MCI. We noticed that you presently have an account with MCI and we wanted to let you know that we'll be offering 'one plus' service in your area starting December 10th. We'd like to verify your address."

The nice lady then read us our address, which was one hundred percent correct. She then said another person would call us to confirm this information. That call came within minutes and was almost identical in content.

A couple of weeks later we got another one of those calls on another of our lines that had an MCI account attached to it. But this time the second call never came.

In early December, equal access came to our phone lines. We decided to check the status of those two lines that had gotten the calls. We dialed 1-700-555-4141. And guess what? They had both been claimed by MCI. Surprised? We weren't. In fact, when those calls come in, we *expected* them to try and pull this scam we'd heard so much about. They made one big mistake though -- they tried it on us.

We always listen very carefully when phone companies call us. And we can say very definitely that MCI never asked us if we wanted to choose them as our long distance carrier. All they asked us to do was to verify our address.

OK, so it was a sloppy representative. Maybe even a corrupt one. How can you condemn an entire company because of the actions of one person? That's quite easy. It happened more than once. Different representatives called different phone numbers and gave the same little speech. And we've found out that other people have gotten the same treatment. This indicates to us that these representatives are reading a script that tells them *not* to ask the customer whether they actually *want* MCI's "one plus" service. Address verification, after all, is a much less controversial issue.

Perhaps MCI feels they're taking a calculated risk here. They only seem to make these calls to people who already use MCI in some form. Maybe they feel these people won't raise a fuss when they discover who their long distance company is. In fact, they may never even discover that MCI is their carrier since they most likely have been getting MCI bills in the past. Remember, these are people who have already been using MCI's services.

Regardless of whether or not it pays off, it's distressing to see such dishonest tactics on the part of a major company.

This isn't our only gripe with MCI. We had been using an account on MCI's 950-1986 dialup. In November we paid the bill a few days late (it was under \$10). Well, lo and behold, they disconnected our code without *any* warning. When we asked them to reconnect it, they said they would have to handle our payment for 10 days first. Ten days went by and the code was still down. We asked again. This time, they said they were phasing out that service, so they couldn't reconnect us. But they came up with a bright idea. We could use our 14-digit MCI Card code instead of our old 5-digit code. "It's just as easy to remember," they said.

Clearly, they have the right to phase out their services and replace them with less desirable ones. But once again, it's the way in which they did it. MCI jumped at the first opportunity to take away our old code instead of being up front and letting their customers know that as of a certain date this service would be terminated. Being sneaky about it doesn't do anyone any good.

The Real Scam

We've saved the best for last. When we discovered that MCI had selected themselves as our long distance carriers, we decided to experiment a little. One of our experiments involved trying to make an operator assisted call ("zero plus") on an MCI line. MCI doesn't offer operator assisted services. So we were curious as to

A Lot of Explaining To Do

what would happen when we tried to do this.

What happened was a big surprise. We got the same little fading dial tone that we got on AT&T -- in other words, the prompt to enter our AT&T calling card number. We entered the card number and were astounded to hear a recording say, "Thank you for using NTS."

NTS? Who the hell were *they*?! And what were they doing accepting AT&T calling card numbers on MCI lines?

We'll skip all of the drama and simply tell you what we found out. NTS is an Alternate Operator Service (AOS) company. They handle calls from hotel rooms and privately owned payphones. Their rates are often double those of AT&T. And it seems that in various parts of the country, MCI has a clandestine relationship with these people. We say clandestine because we're in the habit of reading all of the literature from every phone company that serves our area. And nowhere has this little "service" been mentioned. We have yet to find anyone in MCI who is even aware of this arrangement. On the other hand, NTS (based in Rockville, Maryland) is quite proud of the MCI connection. All of the NTS operators (who can trick anyone into believing they're really from AT&T) are aware that they provide service for MCI "zero plus" customers.

Why does MCI use an AOS? We can't imagine. But we can tell you the effects. If you decide to call someone collect from your phone and MCI happens to be your long distance carrier, the person who accepts on the other end will wind up with one hell of a surprise when they get the bill. You'll be the one getting the surprise if you forget that MCI doesn't have operators and you attempt to place an operator-assisted or calling card call through them. The most likely scenario, though, would be something like this: you visit a friend and need to make a phone call from his house. Since you don't want to make your friend pay, you dial it "zero plus" and bill it to your calling card. How are you to

know that your friend selected MCI as his long distance carrier and that you've just been swindled by an AOS? Perhaps MCI's new slogan can be: "We bring the thrill of hotel phones right into your own home!"

Now we should point out that this "NTS Connection" doesn't work everywhere. In some areas you get recordings when you try to make "zero plus" calls using MCI. We need to know where it does work. You can find out at no charge by dialing 10222-0 followed by a ten digit phone number (you can use your own). If you hear a fading dial tone, it means you're about to be connected to NTS. You can stay on and ask a whole lot of questions if you want. Let us know if it works in your area. (You can do the above even if MCI isn't your primary carrier -- the 10222 routes the call to MCI. You must have equal access in your area in order to try this.)

There's really not much more to add. We are demanding a public statement from MCI addressing the issues of signing up unsuspecting consumers and billing their own customers exorbitant rates for operator-assisted calls without telling them. We don't expect to ever get such a statement.

Several years ago, we printed a story about MCI's electronic mail system, MCI Mail, which had a policy of terminating accounts that had received mail not to MCI's liking. We called it a flagrant invasion of privacy to peruse the mail of their own paying subscribers. The president of MCI indicated that he couldn't care less.

So all we can say right now is that it would be a very good idea to **boycott** MCI for all of the above reasons. A company that resorts to such devious methods of making money and that treats its customers so shabbily is not worthy of the historical significance its founders achieved.

We would appreciate it if this article was spread around in whatever ways possible.

A HACKER'S GUIDE

by Red Knight
Phreakers/Hackers Underground
Network

Brief History of UNIX

It's because of Ken Thompson that today we're able to hack UNIX. He used to work for Bell Labs in the 60's. Thompson started out using the MULTICS OS. It was later eliminated and Thompson was left without an operating system to work with. He had to come up with something really quick. He did some research and in 1969 UNIX came into being. It was a single user system and it didn't have many capabilities. In a combined effort with others he rewrote the version in C and added some good features. This version came out in 1973 and was made available to the public. This was the beginning of UNIX as it's presently known. The more refined version of UNIX is known as UNIX system V. It was developed by Berkeley University and it has unique capabilities.

Various types of UNIXes are CPIX, Berkeley Ver 4.1, Berkeley 4.2, FOS, Genix, HP-UX, IS/I, OSx, PC-IX, PERPOS, Sys3, Ultrix, Zeus, Xenix, UNITY, VENIX, UTS, Unisys, Uniplus+, UNOS, Idris, QNIX, Coherent, Cromix, System III, System 7, sixth edition.

Hacking UNIX

I believe that hacking into any computer requires knowledge of the operating system itself. Basically what I will try to do is get you to be more familiar with UNIX operation and its useful commands.

Error Messages (UNIX system V)

Login incorrect - an invalid ID and/or password was entered. This means very little. In UNIX there is no way of guessing valid user ID's. You may come across this one when trying to

get in.

No more logins - will happen when the system won't accept any more logins. This could mean the system is going down.

Unknown ID - will happen if an invalid ID is entered using the (su) command.

Your password has expired - This is quite rare. Reading the etc/passwd will show you at what intervals it changes.

You may not change the password - The password has not yet aged enough. The administrator sets the quotas for the users.

Unknown group [group's name] - occurs when chgrp is executed and the group doesn't exist.

Sorry - indicates that you have typed in an invalid super user password (execution of the su).

Permission denied! - indicates you must be the owner or a super user to change the password.

Sorry [# of weeks] since last change - this will happen when the password has not aged enough and you try to change it.

[directory name]: no permission - you are trying to remove a directory for which you have no permission.

[file name] not removed - trying to delete a file owned by another user that you don't have write permission for.

[dirname] not removed - ownership of the dir that you're trying to delete is not yours.

[dirname] not empty - the directory contains files so you must delete the files before executing the rmdir.

[command] not found - you have entered an invalid command which is not known to UNIX.

can't execute pwd - something's wrong with the system and it can't execute the pwd command.

TO UNIX

cannot chdir to .. - (.. means one level up) permission is required to execute pwd above the current directory.

can't open [file name] - you defined the wrong path or file name or you have no read permission.

cp: [file name] and [file name] are identical - self-explanatory.

cannot locate parent directory - occurs when using mv.

[file name] not found - file which you're trying to move doesn't exist.

You have mail - self-explanatory.

Error Messages

(Basic Networking Utility)

cu: not found - networking not installed.

login failed - invalid ID or password or wrong number specified.

dial failed - the system never answered due to a wrong number.

uucp completely failed - did not specify file after -s.

wrong time to call - you called at a time not specified in the systems file.

system not in systems - you called a remote not in the systems file.

UNIX Logon Format

The first thing you must do is switch to lower case.

Here is what you will see (sometimes there will be no system identifier).

AT&T UNIX Sys VR3.0 (example of a system identifier)

login:

or

Login:

Any of these is a UNIX. This is where you will have to guess at a valid user ID. Here are some that I have come across: glr, glt, radgo, rml, chester, cat, lom, cora, hlto, hwill,

edcasey, and also some containing numbers: smith1, mitu6, and some containing special characters like bremer\$, j#fox. Login names have to be 3 to 8 characters in length, lowercase, and must start with a letter. In some XENIX systems one may login as "guest".

User Level Accounts

In UNIX they have what are called accounts. These accounts can be used at the "login:" prompt. Here is a list:

sys

bin

trouble

daemon

uucp

nuucp

rje

lp

adm

listen - if starlan is installed

*"Super user accounts
make UNIX worth
hacking."*

Super User Accounts

And then there are super user accounts which make UNIX worth hacking. These accounts are used for a specific job. In large systems they are assigned to users who have a responsibility to maintain subsystems. They are as follows (all lower case):

root - this is a must. The system comes configured with it. It has no restrictions. It has power over every

HACKING AWAY

other account.

unmountsys - unmounts files.

setup - system setup.

makefsys - makes a new file.

sysadm - allows useful commands (doesn't need root login).

powerdown - powering system down.

mountfsys - mounts files.

checkfsys - checks files.

These accounts will definitely have passwords assigned to them. These accounts are also commands used by the system administrator. Here are some examples of accounts I have seen:

cron

uuhelp

usenet

anonuccp

news

network

bellboy

lp

vector

guest

games

ninja

vote

warble

sysinfo

Password Entry

After the login prompt you will receive a password prompt:

password:

or

Password:

Enter the password (it won't echo). The password rule is as follows: each password has to contain at least six characters. The maximum is eight. Two of these have to be letters and at least one has to be a number or a special character.

The letters can be in upper case or lower case. Here are some of the passwords that I have seen: Ansuya1, PLAT00N6, uFo/78, ShAsHi..., Div417co.

The passwords for the super user accounts will be difficult to hack. You can try the accounts interchangeably (example: login:sysadm password:makefsys). It really could be anything. The user passwords are changed by an aging process at successive intervals. The users are forced to change it. The super user will pick a password that won't need changing for a long period of time.

You Have Made It!

The hard part is over and hopefully you have hacked a super-user account. The next thing you'll probably see is the system news:

login:john

password:hacker1

System news

There will be no networking offered to the users till August 15, due to hardware problems.

\$

\$ is the UNIX prompt which means that UNIX is waiting for a command to be entered. I will use this throughout the article to show outputs, etc. (it's not a part of the command). # means you're logged in as root (very good).

How UNIX is Made Up

UNIX is made up of three components: the shell, the kernel, and the file system.

The Shell

The shell is a high level language. It has two important uses. It acts as a command interpreter. For instance, when using commands like cat, who,

ON UNIX

ls, etc., the shell is at work figuring out whether you have entered a command correctly or not. The second most important reason for the shell is its ability to be used as programming language. Suppose you're performing some tasks repeatedly over and over again. You can program the shell to do this for you.

The Kernal

You could say that the kernal is the heart of the UNIX operating system. The kernal is a low level language lower than the shell which maintains processes. The kernal handles memory usage, maintains the file system, the software, and hardware devices.

The File System

The file system in UNIX is divided into three categories: directories, ordinary files, and special files. (d,-)

SEE FIGURE A.

/unix - is the kernal

/etc - contains system administrator's files. Most are not available to the reg-

ular user (this directory contains the /passwd file).

Here are some files under the /etc directory:

- /etc/passwd
- /etc/utmp
- /etc/adm/sulog
- /etc/motd
- /etc/group
- /etc/conf
- /etc/profile

/dev - contains files for physical devices such as the printer and the disk drives.

/tmp - temporary file directory.

/lib - directory that contains programs for high level languages.

/usr - this directory contains directories for each user on the system.

Example of a list of files under /usr:

- /usr/tmp
- /usr/lib
- /usr/docs

Basic structure

(/) - this is an abbreviation for the root directory.

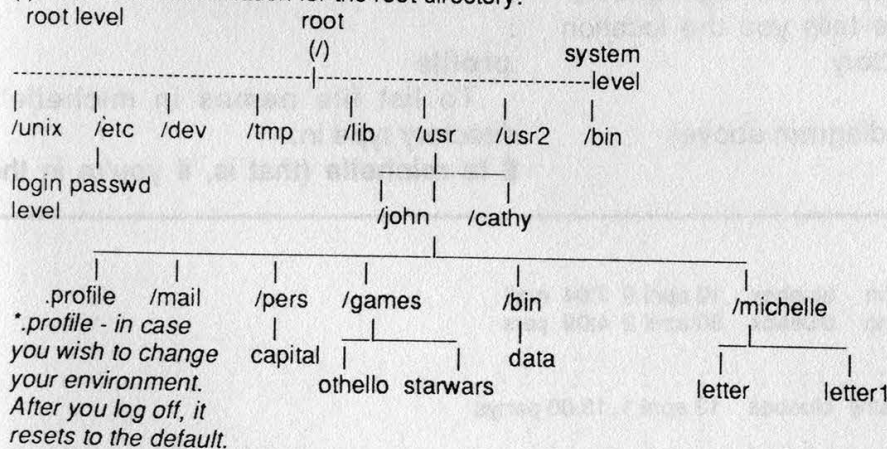


FIGURE A

HACKER'S GUIDE

```
/usr/news
/usr/spool
/usr/spool/lp
/usr/lib/uucp
```

/bin - contains executable programs (commands)

The root also contains:

```
/bck - used to mount a backup file system.
/install - used to install and remove utilities.
/lost+found - this is where all the removed files go. This dir is used by fsck (1M).
/save - a utility used to save data.
/mnt - used for temporary mounting.
```

Local Commands Explained in Detail

At the UNIX prompt, type the `pwd` command. It will show you the current working directory you are in.

```
$ pwd
/usr/admin - assuming that you have hacked into a super user account.
$
```

This gives you the full login directory. The `/` before tells you the location of the root directory.

or
(refer to the diagram above)

```
$ pwd
```

```
/usr/john - assuming that you have hacked into John's account.
$
```

Now let's say you wanted to move down to the michelle directory (you own this) which contains letters. You would type in:

```
$ cd michelle
or
$ cd usr/john/michelle
$ pwd
/usr/john/michelle
$
```

To go back one directory, type in:

```
$ cd ..
or to go back to your parent directory, just type in "cd".
```

To list file directories, assuming you are in the parent directory:

```
$ ls /usr/john
mail
pers
games
bin
michelle
```

This won't give you the `.profile` file.

To view it type:

```
$ cd
$ ls -a
```

```
:
```

```
:
```

```
.profile
```

To list file names in michelle's directory type in:

```
$ ls michelle (that is, if you're in the
```

```
$ ls -l
total 60
-rwxr-x--- 5 john bluebox 10 april 9 7:04 mail
drwx----- 7 john bluebox 30 april 2 4:09 pers
:
:
:
-rwxr-x--- 6 cathy bluebox 13 april 1 13:00 partys
:
:
$
```

FIGURE B

TO UNIX

"john" directory)

```
$ ls /usr/john/michelle (parent directory)
```

ls -l

The ls -l is an important command in UNIX. This command displays the whole directory in long format. Run this in the parent directory.

SEE FIGURE B.

The total 60 tells you the amount of disk space used in a directory. The -rwxr-x--- is read in triples of three. The first character (-, d, b, c) means the following: - is an ordinary file, d is a directory, b is a block file, c is a character file.

The r stands for read permission, w for write permission, x for execute. The first column is read in three triples as stated above. The first group of three (in -rwxr-x---) after the "-" specifies the permission for the owner of the file, the second triple is for the groups (the fourth column), and the last triple indicates the permissions for all other users. Therefore the -rwxr-x--- is read as follows: the owner john has permission to read, write, and execute anything in the bin directory but the group has no write permission to it and the rest of the users have no permission at all. The format of one of the lines in the above output is as follows:

file type/permissions, links, user's name, group, bytes taken, date, time when last renewed, directory or file name.

chmod

The chmod command changes permission of a directory or a file. Format is chmod who(+, -, =)(r, w, x). The who is substituted by u-user, g-group, o-other users, a-all. The + means add

permission, - means remove permission, = means assign. Example: if you wanted all other users to read the file named mail, you would type:

```
$ chmod o+r mail
```

cat

Now suppose you wanted to read the file letter. There are two ways of doing this. First, go to the michelle directory. Then type in:

```
$ cat letter
line one ...\
line two ...the output of letter
line three../\
$
```

or if you are in the parent directory, type in:

```
$ cat /usr/john/michelle/letter
```

and you will have the same output. Some cat options are: -s, -u, -v, -e, -t.

Special Characters in UNIX

* - matches any number of single characters. (Example: ls john* will list all files that begin with john.)

[...] - matches any one of the characters in the [].

? - matches any single character.

& - runs a process in the background leaving your terminal free.

\$ - values used for variables also \$n - null argument.

> - redirects output.

< - redirects input to come from a file.

>> - redirects command to be added to the end of a file.

| - pipe output (Example: who|wc-l tells us how many users are online).

passwd

Password changing seems to be a big thing among some. To change the password, one would use the "pass-

(continued on page 40)

Account Number: 516 751-2600
 October 19, 1988
 Page 1

Last page

Operator Assistance Network

This portion of your bill is provided as a service to Operator Assistance Network. There is no connection between New York Telephone and Operator Assistance Network. Operator Assistance Network provides operator-assisted telephone service which may originate from certain hotels, hospitals, pay telephones, or other locations. Charges for these calls are set by Operator Assistance Network and are not determined by New York Telephone.

Helpful numbers

Billing inquiries call New York Telephone (516) 473-9950
 For changes in Operator Assistance Network service call 1-800-622-4027

Itemized calls

Convenience calls (collect, third number and other operator assisted)

No.	Date	Called from	Called to	Time	Rate	Type	Min.	Amount
1	AUG 29	Calling number 751-2600 LAS VEG NV 702 735-4051	STONYBROOK NY 516 751-2600	11 57 AM	DAY	Collect	7	\$ 5.24
								Sub Total
								5.24
								Itemized calls Total
								5.24
								Federal Tax (3%)
								.16
								Total
								\$5.40

IT TOOK A LOT OF GALL for someone to call us collect and somehow convince an untrained operator that we had accepted the charges and then apparently talk to our answering machine for seven minutes. It also takes a lot of gall for an Alternate Operator Service company like the above to charge the astronomical rates they do, let alone come up with an official sounding name like "Operator Assistance Network". When we first saw that line on the phone bill, we thought it was some kind of tax or surcharge. That's why we decided to expend a little gall of our own and expose the entire sordid affair, phone numbers and all.

how to hear phone calls

You too can be nosy and listen in to other people's telephone calls with a radio receiver. Depending on what kind of radio(s) you have, here are the things you can pull in:

Short Wave Radio: You need a general coverage receiver that is capable of receiving in single sideband mode (SSB) or has a BFO mode. Your antenna can either be the whip antenna on the radio or a long piece of wire, ten to fifty feet, running around your home or better yet, outside to a tree or pole. You will be able to tune ship to shore telephone calls within the following frequency bands (all numbers in kilohertz):

4357-4434,
6506-6521,
8718-8812,
13100-13197,
17232-17356,
22596-22716.

These frequencies are the shore station, which usually broadcasts both sides of the conversation. Transmissions are in upper sideband (USB) mode. Conversations may roll in from all over the world, especially at night, and will be in many different languages.

Some shortwave receivers can tune all the way down to the AM band. If yours does, check 1690 to 1770 kilohertz, where the old cordless tele-

phone base channels are located.

Standard UHF/VHF Scanner: You can pick up cordless phones in your immediate vicinity, IMTS (old style car phones) in your general area, and airplane phones flying overhead. For the base stations, you'll usually hear both sides of the conversation, although sometimes the mobile caller won't be audible and you'll just have to imagine what they're saying. Use either the whip antenna on your scanner or buy an outdoor scanner antenna. These frequencies are listed in megahertz:

Cordless phones
46.610 to 46.970
IMTS car phones
152.510 to 152.810
(base stations)
Airplane phones
454.025 to 455.000
(land stations)
459.025 to 460.000
(airplanes)

The ECPA bans listening to car telephones. Cordless and airplane phones are governed by section 605 of the Communications Act of 1934, which says you can listen all you want as long as you do not divulge the information to anyone else or use it for profit.

800 Mhz Scanner: Newer

phone calls are

scanners cover all of the above mentioned scanner frequencies as well as the 800 Mhz cellular telephones (provided the manufacturer hasn't locked out the capability). Note that cellular telephones are of a wider bandwidth than most other scanner signals, and the average scanner may lose the peaks of some words, especially a high-pitched women's voice or a person screaming. For an antenna, start with the whip antenna on the scanner: slide it in all the way so that it is as short as possible (800 Mhz is a small wavelength, so shorter antennas are called for). Experiment also with angling the whip for better reception. Or purchase an outdoor antenna that is tuned for 800 Mhz. Or purchase a car cellular antenna and mount it outside your window (or on your roof).

870.000 to 890.000

(base stations (cells) for the standard cellular system.)

890.000 to 896.000

(base stations for the extended cellular channels. Not in widespread use yet.)

As mentioned before, the unenforceable ECPA bans listening to cellular telephones.

Old Television Set: Some of the frequency space for cellular telephones used to be UHF TV channels 79 through 83. That's why newer TV sets have less UHF channels. If you don't have an 800 Mhz scanner yet, make sure there's an antenna attached (either the UHF loop or the UHF lead-in from an outdoor antenna), and try tuning across those channels. A continuous tuning knob will work better than the click stop kind. Cellular telephone calls on your TV set could be considered unwanted interference, but the law mandates that you turn your TV set off as soon as you realize that you are receiving protected communications.

Standard AM Radio: Haven't got any fancy radio equipment and don't want to buy any? If your neighbors are using the older models of cordless phones, you might be able to pick up the base channel at the far end of the AM dial (past 1600).

Country	Phone Access Number	Customer Service Number
Starting October 1, 1988:		
Australia	0014-881-100	0014-800-125-682
Belgium	11-00-12	11-65-80
Denmark	0430-0022	0430-0030
France	19*-00-19	19*-05-90-27-21
Netherlands	06*-022-91-22	06*-022-10-22
Sweden	020-795-922	020-795-912
Starting November 1, 1988:		
United Kingdom	0800-89-0222	0800-89-1852

*Await second dial tone.

in the air

WHAT MIGHT YOU HEAR ON A CAR PHONE? WE'RE NOT SAYING THAT ANYONE ACTUALLY LISTENS TO THIS STUFF AND THEN WRITES IT DOWN FOR MAGAZINE ARTICLES, BUT IF THEY DID, IT MIGHT LOOK LIKE THIS....

> I think that...the part of the problem is that they got -- they got a buyer for, for Kent. We'll just make it back in the commission for Kent. Now you understand that?

< Who'll just make it back?

> Huh?

< Who?

> Jerry, Larry, and you.

> What do you do with a group like that? You know. I mean what, I mean what, what do you with somebody like the deal?

< I don't know what you do anymore. I mean, the music is changing so radically it's hard to keep up.

> Yeah.

< It's hard to find out what to do it anyway.

> Yeah.

< You know?

> Yeah. Yup. How's the kids?

< How're the kids?

> Yeah.

< Kids are great, Bill.

> You got 'em a job yet?

< What?

> You got 'em a job yet?

> I feel bad for me. I feel bad for both of us. My heart hurts too. I love you.

< Who loves you?

> (osculating noises) I would kiss it if I could kiss your heart.

< (giggle)

> It was beating like a little thumper before.

< Really?

> (more osculating noises)

< God....

> A nice little orgy.

< Umm, I know. God you feel great down there tonight.

> Yeah I had it in, I was holding it differently.

< Oh. Felt wonderful.

> Did you notice that?

< Yeah. I told you it felt great, whatever it was you were doing.

> Uh huh.

< I could tell it was different, but I don't know what it, you're doing.

> Yeah. It was definitely different.... (pause) Want me to tell you what I did?

do not attempt

- < Sure.
- > I like squished it with my left hand. And I just left a space open for that leeeetle clitoris to stick out.
- < You were squishing it? Cause it felt like you were pulling it apart?
- > Well, at the same time I was, had the two fingers pulling it apart but the bottom of my hand, was like, squashing it in.
- < Uh, well, that felt great. (pause) Oh. God I was horny.
- > You're horny now?
- < No, I was horny.
- > Oh.
-
- < Which one..
- > No, the one we run last year was our art deco.
- < Yeah?
- > This is totally different. We're not talking about the same one. The one --
- < Totally different is the difference between an eagle and an automobile. They're totally different.
- > It's not.
- < Sheesh. You're talking about a yoke treatment that comes down like a V, one is art deco, one is floral....
- > Okay, then you know what I'm talking about.
- < Of course I know, but you know, you're looking at it like through a microscope....
- > No....
- < And you're going to say it's entirely different but if you stand back and say "Hey...."
- > Alright, watch what happens with this one....
- < Well, I think we could do well with it, but it really is basically the same concept.
- > I don't think so, not at all.
- < You don't think it's the same concept?
- > No, nope.
- < Nah, then you're losing it.
- > No I think they're all --
- > -- and when can you give me an answer?
- < Right.
- > And it was very nice. But you can't, I mean she was on the phone with Brian this morning, and, and suddenly it was, it was the money thing. And I got on the --
- < What's the money thing?
- > You know, and I got on the phone with him and I said Brian, just, you know, come over here and look!
- < But you could take almost

this at home

everything.

> I know.

< You know -- it's also bothering you in the background.

> No.

< Oh yeah.

> Not with Brian.

< Brian, he knows Brian all so well.

> Yeah, but Brian and he did not get along very well.

< Yeah, but Bobby seems has been to his head, you know, 'Be careful, you're gonna get screwed.'

> Yeah....

< You know, you know, uh ya know you hear it from, you know, either I get screwed or you're gonna get --

> Oh, I know, I know, but you know on the other hand after you talk to him for a few minutes he's coming over at one o'clock to work.... Howard?

< No bullshit about it.

> Yeah, but, uh, you know I mean they see, they see a lot of work going on down it's going to change people's attitudes.

< You know he -- if he wants to jerk -- you know, you know he could play all the

routines they want, construction's slowing down right now.

> I know.

< And if they want -- you know, uh.... Lexington Avenue --

> I know.

< And Bergen Avenue.

> I know.

< And Old Bergen Avenue.

> I know.

< Uh, I, they just gotta understand, uh you know, I mean I gotta, what I gotta do is start going out there more to see him then.

> Uh huh.

< And, you know, doing my routine and say I know how to do very well with that.

> Right, exactly.

< They would give me a fucking break, we have some closings, we'll pay you, you know we're right around that time, we're closing, you just gotta wait a little while.

> That's right, that's right.

THIS IS THE FIRST IN AN OCCASIONAL SERIES ON POSSIBLE CONVERSATIONS THAT ANYONE COULD OVERHEAR. IF THIS HAD BEEN AN ACTUAL CONVERSATION, LOOKING AT THIS ARTICLE WOULD BE ILLEGAL.

Letters For

Some Ideas

Dear 2600:

After month's of agonizing over 2600's financial plight, I've figured out a way to return to the monthly format and solve another great problem that plagues BBS's all over the nation. How many times have you logged onto your favorite BBS and seen some message like this: "It has come to my attention that someone else is using *my* name, 'The Grim Reaper', on other BBS's. Well, whoever you are, I'm the *real* Grim Reaper. I was The Grim Reaper months before you came around. You better not use my name any more, or I'm gonna kick your \$#&*@ ass!!! You better think of a new name dude!!!"

Well, the obvious solution to this common dilemma is to have a sort of "name registration", where individuals can register their alias with an authority -- kind of like your given name when you're born. And who else would be the most likely authorization but the hackers' and phreaks' choice -- 2600! Think about it! You could charge each registration a nominal fee, like \$3. For that \$3, you will give the person a registration certificate, saying that he is the only one authorized to use a particular

alias within a given limit, say, an area code. The person could get some little certificate to hang on his wall, and maybe even a patch to sew on his jacket.

So the next time the loser user logs onto the BBS, he can now proudly assert: "By the power of 2600, I am the only Grim Reaper within the 212 area code. I am the only one certified and authorized to use that pseudonym. So be gone, you pagan!"

So, whadaya say? 2600 could be put into the black, and we would no longer have to put up with dueling 14 year olds. We have a unique opportunity to help solve the hackers' two most serious problems.

No thanks. There must be a better way to raise funds than to play big brother to dueling 14 year olds. Besides, how in the world would the user be able to prove that he/she was the one with the certificate hanging on their wall? Computers still offer a degree of anonymity. Let's all try to enjoy that while we can.

Articles & Boards

Dear 2600:

After having received your volume 4, number 10 issue, I was truly amazed! It's great to

Winter Reading

see a publication that is straightforward and informative. It wittingly caters to the novice, as well as those of us who hopelessly suffer from occasional periods of "hack attacks". Good job!!

I would like to inquire about submission of written articles, relevant computer news, newspaper stories, and the like. I believe I have or can obtain enough data to "publish" at least one article on a minimum quarterly basis. Also submittable would be a collection of "postings" from the area networks which would be of worth to your magazine.

Next on my list is the hope of being allowed to operate a Greater New Orleans branch of 2600 Magazine BBS. I know of *many* people and users who would be more than happy to benefit by logging into a system like such. A BBS of the like would offer its users a wealth of information that would otherwise be inaccessible, or worse yet, unnoticed! As I soon will have a phone installed with a few *extremely* advantageous services such as call forwarding and call transferring, I will also be able to link users to systems that would be out of their reach *but within mine!* I think that the combination of what a 2600 Magazine BBS

could offer, plus a bit of effort on my part, would bring about great results.

SW

You can contact us with your BBS ideas by calling 516-751-2600. We're also always asking for unsolicited articles, so if you have something you think we might publish, send it in.

Need Info

Dear 2600:

I understand that the Telecaption Adaptor II available from Sears can be extended with a few parts to have an RS232C serial output port for a computer. I would like to find out how to do such a modification so that the TV subcaption output can be displayed on a Teleprompter with RS232 input. This would allow people who are both hearing and sight impaired to understand TV. My grandmother cannot see the tiny letters that the TCA II generates on the screen. I would appreciate any information on how to accomplish this modification.

Handel

AT&T Nightmare

Dear 2600:

Our small liberal arts college recently switched over from its

The Winter

old crossbar system to the AT&T System 85 early this year. In the old days, you subscribed to Wisconsin Bell (like all Wisconsin residents), had your name in the phone directory, were available through directory assistance, and could use your long-distance service with the 1+ option. That has changed since then. If technology is supposed to make life easier, it doesn't and it also makes it a hell of a lot more expensive.... To make a long distance call, we now have to dial the 800 port (I use Sprint) and use a calling card to place the call. For those of you who use software for your modems, try programming a 20+ sequence! Then we also are charged a 50 cent surcharge for placing the call! And if you're like me, that really adds up. We are unable to call 950's, "toll free" Wisconsin Bell lines, and we are unable to turn off call waiting for an incoming call. Good if you are trying to run a BBS from your dorm room. There are only 37 outgoing lines, and 27 incoming. So during normal business hours (the school's business office is also on the system), you will be unable to place a call! Someone from AT&T also forgot to program all of the reachable prefixes in our area! Even some of

our faculty cannot call home! For a system that is supposed to be "smart", it sure isn't. If I were to call myself using the prefix that the school is accessible through, the phone system doesn't even know to just use an internal switch. Instead it goes ahead and wastes an outgoing and incoming line while I talk to myself. So to prove to the school that something needs to be done, we're getting 37 people to call themselves during busy business hours, and make the system paralyzed...for about 4 hours. That should teach them what they refuse to listen to. Like all systems, no one cares until it happens to them....

**Cray-Z Phreaker
Skunk Works**

The bug you're about to exploit is probably the easiest part of the system to fix. All they have to do is block out that exchange like they've blocked out others. But the point is you have to get the college and the phone company to listen to you, the end user. You must do whatever you see fit. This means being loud and specific as to what problems you're faced with. Remember, you have the same right to telephone service as anyone else in this country. Being at a col-

Letters Column

lege does not mean you're signing away this right. Demand answers and if you don't get them, make sure everybody knows it.

And a message to AT&T: This is the second time in as many issues that we've heard major complaints about your System 85. Last time it was the House of Representatives. Who will it be next?

Call Forwarding

Dear 2600:

I'm hoping you may be able to answer some questions regarding the phone company's availability of call forwarding.

As it stands, in order to activate call forwarding, you must have the service on your line and you must activate it from that line. It must be deactivated from the same phone that it was activated on.

My question is this: is it possible to forward Phone "A" to Phone "B" from Phone "C"? Also, is it possible to have a pay phone forwarded to your location?

JH

There are remote call forwarding devices available that allow you to change the number you're forwarding to and to cancel call forwarding from a remote location. We talked

about these in our last issue. So far we haven't seen a phone company offer these services. Regardless of who offers it, though, there is another potential security risk here.

With regards to using forwarding on a payphone, there are two answers. The first is no. That is, according to the phone company. After all, why would anyone want to use forwarding on a payphone? It's simply not possible. The other answer is yes. Of course, it's possible. Hackers have done it by using the phone company's computer. And we don't doubt that law enforcement has made use of it on occasion. What better way to trick a drug dealer or kidnapper calling a payphone?

Observations

Dear 2600:

Seeing how you have published updates to the 800 exchanges that are owned by IC's, here are some 800 exchanges that belong to other companies, as well as some of the same companies (MCI, Sprint, etc.). These all work from my NPA, and I live in the midwest. I know that one carrier (LYTEL) is a re-seller of long distance lines to FG-B carriers in my area. Anyway, the list:
800 + NXX

We Really Like

373 - Teleconnect
383 - Teleconnect
456 - MCI
472 - AT&T
589 - LYTEL
636 - Conquest Long Distance
668 - AT&T
686 - Conquest Long Distance
728 - Teleconnect
747 - Teleconnect
798 - Teleconnect
829 - Sprint
869 - Sprint
873 - MCI

These are the exchanges that I have found that were not listed in any issue of *2600* under any company. There may be more, since I compiled this list a few months ago. Also, Teleconnect in this case is not the same company that runs *Teleconnect Magazine*, I am told. I can usually tell by listening if the exchange is owned by an IC, as there seems to be more noise and static on the connections and in the background than there is with AT&T 800 numbers. Also, in my area at least, the connection time for an AT&T 800 number is less than for an IC-owned 800 number. Western Union's service used to be such poor quality in my area that when I dialed 10220# (their equal access override), I could hear the noise being cut for ANI and called number out-

pulsing. This also was the same for Allnet.

Speaking of Allnet, I am a legal customer of theirs, with dial-up service. When I got my authorization notice in the mail, I discovered that my code had been put in on Allnet's 800, 950, and local FG-A dialups. On the 950 and local FG-A node, I could use my 6 digit code "as is", but with the 800 "Travel-Mate" service, I must enter my 6 digit code, plus my three digit PIN. (By the way, Allnet used to use some type of formula to derive customers' PIN numbers. This formula used part of the customer's exchange as the first digit of the PIN. I am just mentioning this for the sake of information, as they no longer use this method, according to customer service.) I am less than happy with Allnet's service -- they are raising prices in my area for both dialup and equal access dialing. Also, they cannot seem to get their records straight. Somehow I was signed up with Allnet as my PIC even though I did not choose them. I talked to customer service about it as soon as I found out and they told me the problem would be fixed. Soon afterwards, I received a notice in the mail telling me that I had been disconnected

Getting Your Letters

from Allnet. However, to this day, I am still connected with Allnet and they cannot get the bills straight. They send the bill for 1+ to my address for dial-up bills. I have called them several times and still they cannot fix this.

Also, to top things off, we still received the charge from our local BOC to pay for the disconnection from Allnet even though we are still connected. I have called customer service a number of times and they don't seem to want to help. I have considered dropping Allnet because of the several things they have done, but I am still a customer of theirs. The only good thing about Allnet is that they have a 45 second buffer zone that is used when a call is connected. So if you can keep a call's time less than 45 seconds, it won't show up on your bill. I imagine that sooner or later they will get the equipment to detect answer supervision, but it looks like it will be later.

In the Spring 88 issue you published a list of BOC routing and system codes. You asked if anyone knew how to use the Mexico function of RQS. You can use this with a Mexico NPA, such as 905. Just use 905 as the NPA and use two Mexican exchanges in the

exchange information, and RQS will tell you the rate. If you want to try this out, a valid exchange in Mexico is 621. So if you use 905+621 and get the rate information for an intra-office call (to the 905+621 exchange), you will get a local call message.

Also, a note to Telenet ID users, according to Telenet Customer Service, the cost of getting an ID is \$24 a month, \$18 a connect hour, and the bills are itemized (shows that the ID user connected with). So if this information is true, then no wonder Telenet ID's always die when people use them illegally. Also, Telenet has a new type of access management system called TAMS (I am not sure what it stands for) which keeps better track of network usage.

Phantom Phreaker

An increasing number of IC-operated 800 numbers actually have better sound quality than AT&T's. They also have more sophisticated caller identification features.

If you have a letter to send to us, drop it in the mail addressed to: 2600 Letters Department, PO Box 99, Middle Island, NY 11953.

What It's Like To Be

by E. Solomenko
(reprinted from Pravda)

I first came across her when as an inter-city telephone operator in Novosibirsk she tried long and hard but without success to put me through to Ashkhabad.

Her efforts were in vain. "I'm sorry," she said, "I'll try via Mara."

Getting through to Mara was no problem. "Hello, Mara? Can you help me get a line to Ashkhabad?"

The reply was anything but sisterly, "Dial it yourself!" Then they cut her off.

I reflected sadly that the lack of solidarity in Mara was a far more common approach than that of my Novosibirsk guardian angel of the telephone exchange. I remembered how on a previous occasion I had also been trying unsuccessfully to get through to the elusive Ashkhabad, when the operator told me that there was a fault on the line.

Just in case, I decided to try getting through without her help, by dialing direct from the telephone box. Miracle of miracles -- the inter-city code worked and I got through. The operator had told me there was a fault in order to get rid of me.

Ashkhabad was notoriously difficult to get a line to. Yet now her senior colleague was trying again and again to connect me and I could hear her saying to the girl next to her (she had forgotten to switch me off) that she hardly had any voice left from shouting down the line to Ashkhabad.

At long last I heard the voice of

my friend, the artist Durda Bairamov, over the line. We both had to bellow in order to be heard; the line was terrible. The operator's hoarse voice broke in as she started relaying my questions to Durda and his answers back to me. I felt very touched by her concern and just had to find out who she was.

Her name is Valentina Efimovna Vdovina and she works in what they simply refer to as the "inter-city", which is one of the country's largest telephone exchanges, connecting the Urals with Kamchatka and Kuril.

So what is Valentina Efimovna like?

"She's a conscientious worker," said the supervisor, T. Vereshchak. "She never goes home until all the calls that have been booked have got through. Sometimes she sits on into the night long after her shift has gone off duty. We have a lot of good operators here, but we all take our hats off to Valentina."

Then who should come into the room but Valentina herself. About 40 years of age, small with a round face and short hair and very kind, homely eyes. She sits down, obviously tired. Before lunch today she was working on eight calls at once.

Her job isn't exactly a piece of cake. She only has one day off a week and has lost count of the number of national holidays she's spent sitting in front of the switchboard. She works six hour shifts doing what amounts to a juggling act with both hands, connecting and disconnecting plugs from the switchboard.

A Soviet Operator

Then there are the operators' fetters, the earphones with mouthpiece attached. Just try spending a whole shift wearing those things! You soon get bells ringing permanently in your head from the constant noise, and this leads to headaches. Your voice suffers too from the constant shouting to make yourself heard over bad lines.

It is no accident that state legislation allows for early retirement in this job. After ten years in the inter-city, you can retire on full pension at 50. Only a few soldier on for longer. Lilya Gleikh, Vera Raeva, team leader Elsa Vasilievna... Ludmila Ivanovna Gorbatova has served her for almost a quarter of a century and has risen from operator to manager. Other girls come here straight from school and don't last two minutes.

"I'd get out myself," sighed Valentina Vdovina, "but I love my work. I think of it as helping people to meet each other. It's as if I have a hand in their fates, even if only for a minute."

I said that no doubt she overheard many conversations between callers, not on purpose, of course, but how else could she check the quality of line and make sure that they could hear each other, how else could she let them know that their time was almost up?

Whether she likes it or not, the operator must be party to other people's secrets, to their joys and sadnesses. There must be calls from sons returning from the army, calls

to announce the birth of a grandson, to say that somebody has been put in prison or that someone else has had a heart attack.

Sometimes they overhear whole conversations, late at night or on holidays when there are fewer calls going through. During normal working hours they only have time to quickly listen to check that everything is OK. Twenty seconds for each call and on to the next one.

A local call comes in. "Please put me through to Lesosibirsk as quickly as possible, my dear!"

"What number do you want?" Valentina asks.

"I'm afraid I don't know," sobs the voice.

"Please don't cry. Let's try to think how we can find the number. Who do you want to ring there?"

"My daughter's had an accident there," says the woman's tearful voice.

"Don't worry. I'll get through as quickly as I can. I expect the surgical ward of the hospital there will be able to help."

She got through to her colleagues in Krasnoyarsk who gave her a line to Lesosibirsk. From there she got through to the hospital and then to the doctor in charge of the surgical ward.

"Hello, this is the Novosibirsk inter-city exchange. Has there been a young woman admitted following an accident? There has? Hang on a second, I'll connect you to her mother."

Later the mother rang Valentina,

Operating In The

this time crying with relief.

"Thank you my dear. I can't tell you how much you helped me. I don't know how to thank you for all you did."

She doesn't have to thank her. For Valentina the main thing was that the woman found her daughter, knows that she is alive and will get better. That is the best thanks she can get.

In the course of her work she comes across all sorts of different people. Sometimes during the busiest time, when all hell is let loose with ten calls going through the switchboard at a time, you suddenly get an irate caller bursting in saying: "How much longer must I wait? I haven't got all day you know. If you don't pull your finger out I'm going to complain."

"Sometimes we even have difficulties with other operators," explained Ludmila Gorbatova. "We can never get through to the Baku inter-city exchange, the operator on duty never answers. She's either asleep or has gone off somewhere."

"When she does finally answer she shouts something in Azerbaidjani down the phone and hangs up. After which you can never get back through again. We have sent a complaint to the USSR Ministry of Communications and the Baku inter-city exchange, but without result."

Vdovina says that she doesn't very often come across operators like the one in Baku. The other Siberian operators in far eastern

exchanges are all considered to be "one of us" at Novosibirsk.

Valentina started off by working on the Krasnoyarsk district link and now is on the Khabarovsk line which includes the whole of eastern Kazakhstan plus a good chunk of Novosibirsk province.

She is an important link for miners, people working on the gas pipeline project and the agricultural industry. When there is an accident on the pipeline for example, or problems with drilling. When a couple of teams are needed urgently elsewhere -- all this concerns her and she does her best to help.

Let's take, for example, the Novosibirsk Pipeline Construction Trust. She knows as much about their business as its dispatch clerk, Vladimir Ivanovich Golitsin. She knows that the Trust is involved in pipe projects in Belgo and in Lower Tambovka, in Yagodnoe and in Krasnoyarsk.

"Hello, Mr. Golitsin, I'm putting you through to Belgo."

"Hey, Valosha, what about a hello first? How are you nowadays?"

"Hello Vladimir Ivanovich. I can't really talk for long now, the supervisor's here and I'll get told off for chattering!"

The supervisor, Taisiya Aleksandrovna just smiles. "You seem to know the whole country, Valya!"

"Not quite," laughs Valentina, "only half!"

Her son Seriozha more or less grew up in the exchange. When he

U.S.S.R.

was in the fourth class he was told to write a composition called My Future Career. He wrote: "I want to be a switchboard girl." When his mother saw it, she laughed and told him to change it to "man". He looked at her from under his brows and said: "What do you mean, 'man', when they're all girls?"

Over the past two years she has not been very well. The strain of the job is starting to tell. Not long ago she did a break, but now her short,

18 days of holiday are over and she is back at work -- how could they manage without her? She hurries to light her beacon for the Sea of Anxiety, the Sea of Joy, and the Sea of Loneliness.

Tomorrow I shall have to ring Khabarovsk. I'll dial the inter-city and book my call. And how good it will be to hear that friendly voice saying, "Did you book a call to Khabarovsk? Putting you through now."

INTERNATIONAL DIRECT DIAL SERVICE TO IRAN TEMPORARILY SUSPENDED

At the direction of the government of Iran, the Telecommunications Company of Iran has taken action to deny International Direct Dial Service from the world into Iran. Until further notice, all AT&T calls from the U.S. Mainland and Hawaii to Iran must be placed through an AT&T Operator. Effective August 4, 1988, the following new additional minute rates will apply.

OPERATOR-ASSISTED RATES INITIAL 3 MINUTES (ALL DAYS—ALL HOURS)

IRAN	Station Rate, 3 Minutes		\$ 8.87
	Person Rate, 3 Minutes		\$11.83
	NEW ADDITIONAL MINUTE RATES		
	Standard	Discount	Economy
	1pm-2am \$2.19	7am-7pm \$1.88	2am-7am \$1.89

If you have any questions, our representatives are available to assist you. They may be reached by dialing our toll-free number, 1-800-874-4000, ext. 108 (Residence), 1-800-222-0400 (Business).



an interview with

by John Drake

Not much is known about the Chaos Computer Club, except for the abundance of scary "you should hire me because of hackers like them" tales peddled by computer security consultants.

Further hype about the "mythical hacker elite" has also been perpetuated by the worldwide media coverage when a story is picked up by a major news service.

This past fall two members of the Chaos Computer Club were passing through my metropolis. They decided to hunt me down with the little information they had about me. Since they didn't have the street number, the duo spent a night ringing the doorbells up and down the street asking for John Drake.... Their eventual success resulted in this interview.

WHEN WAS THE CHAOS COMPUTER CLUB FORMED?

HMMM, I CAN TELL YOU THE DATE WHEN THE FIRST DATENSCHUEIDER WAS DELIVERED. THIS WAS IN FEBRUARY 1982 AND IT WASN'T PHOTOCOPIED. THE CLUB MUST HAVE BEEN AROUND SINCE '81. THE REASON THERE WERE SOME CONTACTS BETWEEN THE HACKERS WAS THAT THERE WAS AN ARTICLE IN A NEWSPAPER IN GERMANY.... I THINK IT WAS AN AD, IN FACT -- SOME OF US TRYING TO FIND PEOPLE INTERESTED IN COMPUTERS, IN A PAPER CALLED TAGENSIGN -- AN ALTERNATIVE NEWSPAPER. THIS IS HOW THEY GOT TOGETHER. AFTER THIS, I THINK THERE WAS

AN ARTICLE ABOUT HACKERS -- PEOPLE WHO WORK WITH COMPUTERS AND THAT MENTIONED THE DATENSCHUEIDERS. IT WAS IN DER SPEIGAL, LIKE NEWSWEEK HERE, OR TIME, AND SO SUDDENLY MANY PEOPLE PHONED AND WANTED TO GET THE DATENSCHUEIDER. THEN FROM THERE THE SECOND ISSUE OF DATENSCHUEIDER WAS PRINTED A LOT, THEN THE CHAOS COMPUTER CLUB.

WHO THEN STARTED THE CHAOS COMPUTER CLUB?

WAU HOLLAND, HE'S THE ORIGINATOR. HE HAD EXTRA ROOMS AND HE GAVE THE ROOMS TO PEOPLE WHO CAME TO VISIT HIM BEFORE IT WAS A CLUB, AND THE ROOMS OF THE CHAOS COMPUTER CLUB ARE ALSO NEXT DOOR TO HIS PLACE IN HAMBURG.

WHERE DOES PETER GLASER COME IN?

IN 1982, OR EVEN BEFORE THAT...VERY EARLY. PETER GLASER LIVED IN HAMBURG. HE WORKED WITH COMPUTERS FOR A TEXT PROCESSING COMPANY. HE HAD MANY CONTACTS WITH OTHER PEOPLE. SWEN YACKTOFF LIVED WITH HIM. SWEN WAS THE FIRST TO HAVE CONTACTS WITH WAU HOLLAND. HE WAS ONE OF THE FIRST, FAR BEFORE THERE WAS A DATENSCHUEIDER, OR ANYTHING OF THIS KIND, WHO HAD CONTACTS WITH WAU HOLLAND. HE LIVED TOGETHER WITH PETER SO THERE WERE OTHER CONTACTS THERE AND PETER WOULD COME IN CONTACT WITH PEOPLE WHO WERE USING COMPUTERS FOR MORE THAN ONLY TYPEWRITING. SO PETER BECAME A "HACKER". I

the chaos computer club

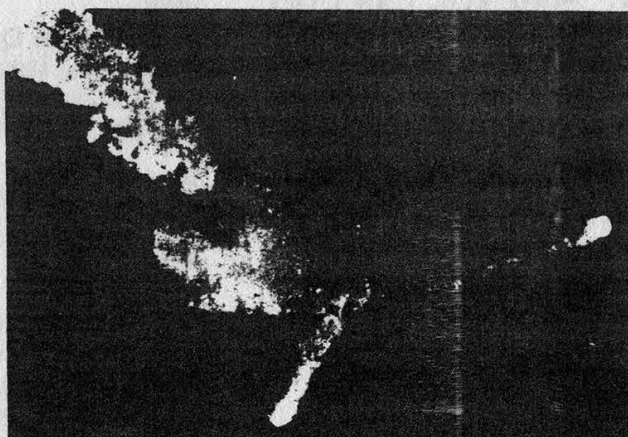
DON'T KNOW IF HE IS REALLY A HACKER...IT'S A SILLY WORD. WHEN HE GOT A MODEM FOR A BIRTHDAY PRESENT FROM SOMEONE FROM THE CHAOS COMPUTER CLUB, FROM THAT TIME YOU ONLY SEE HIS BACK. YES, WHEN YOU WANTED TO COMMUNICATE WITH HIM YOU HAD TO BUY A MODEM YOURSELF. BUT, THAT'S OVER NOW, HE ONLY GOES ONLINE VERY SELDOM.

WITHOUT STRUCTURES. ANYONE CAN COME WITHOUT HAVING TO BE A MEMBER.

How many people receive the DATENSCHAUER?

WE ARE PRINTING TWO THOUSAND, I THINK, BUT ONLY ABOUT 800 TO 1000 ARE ACTUALLY MAILED.

Hamburg (DPA) ... ARIANE - so ein Sprecher der NASA - sei wohl nur deshalb so hervorragend gestartet, weil Hacker im Bootsektor der Rakete Verbesserungen vorgenommen hätten. ...



© 1988 by Arr d'Amblement

Chaos Computer Club, Schwenckestr.85, D-2000 Hamburg 20, Telefon: 040 - 490 37 57, BTX *CHAOS+ Mailboxsystem CLINCH 040 - 651 64 75, via Datex-P 44400090314, GEONET:GE01:Chaos-TEAM

How is the Club set up in relation to DATENSCHAUER?

DATENSCHAUER is the paper of the club.

How is the club organized?

THAT'S VERY HARD TO SAY BECAUSE AS AN OFFICIALLY REGISTERED CLUB IT'S ONLY BEEN A YEAR NOW. BEFORE THEN IT WAS JUST THE CHAOS COMPUTER CLUB. BUT THEN YOU NEED SOMEONE FOR THE BANK ACCOUNT AND YOU NEED A REGISTRATION. IT'S A GALACTICAL CONNECTION

HOW HAS "THE PRESS" LOOKED AT THE CLUB? YOU ALWAYS SEE REPORTS ABOUT THE CHAOS COMPUTER CLUB BREAKING INTO ONE SYSTEM OR ANOTHER....

WHEN YOU GIVE THEM (THE PRESS) SOMETHING TO EAT, THEY ALL COME RUNNING.

Examples?

WHEN YOU HEAR WE HAVE JUST GONE INTO A DATABANK, EVERYONE FROM THE GERMAN PRESS WILL COME AND WRITE ABOUT IT. IN THE BEGINNING THIS WAS VERY FINE AND SOME GOOD ACTIONS CAME ABOUT BECAUSE OF THE BETAX HACK...NOW THERE IS THE

the chaos

NASA HACK WHICH IS VERY FAMOUS.

BUT OFTEN THERE ARE JOURNALISTS WHO THINK "WHAT CAN WE DO IN OUR NEWSPAPER?" AND THEN THEY SAY, "AH YES, SOMETHING WITH COMPUTERS -- LET'S PHONE THE CHAOS COMPUTER CLUB. IS THERE ANYONE HERE WITH THE NUMBER?" THEN THEY PHONE AND SAY, "PLEASE SHOW US SOME HACKING, LET'S SEE HOW YOU DO IT." AND YOU CAN'T DO IT BECAUSE IT IS FORBIDDEN IN GERMANY. IT'S NOT THE REASON WHY THE CLUB EXISTS: FOR JOURNALISTS TO LET PEOPLE KNOW THERE ARE HACKERS.

WHEN A BYTE SOMEWHERE GOES WRONG THEY ALWAYS PHONE THE CHAOS COMPUTER CLUB, BECAUSE THEY THINK WE CAN FIX IT OR WE KNOW WHAT HAS HAPPENED OR WHO DID IT. SOMEONE ONCE TOLD ME THAT BECAUSE OF THE CHAOS COMPUTER CLUB HE HAD SOLD A LOT MORE OF HIS SECURITY SOFTWARE AND HE THANKED US.

IS THE MAIN AIM OF THE GROUP COMPUTER LITERACY OR IS THERE A FACTION INSIDE THE GROUP FOR HACKERS?

THERE ARE MANY DIFFERENT PEOPLE WHO THINK OF MANY DIFFERENT AIMS OF THE CLUB, SOME OF THEM SOCIALLY ACCEPTABLE WAYS OF WORKING WITH COMPUTERS. SOME OF THEM ARE HACKERS BUT NOT ALL OF THEM. WE ARE NOT HACKERS.

IS IT THEN A STRAIGHT COMPUTER CLUB?

NO, IT'S NOT A NORMAL COMPUTER CLUB. IT'S MORE OF A CHAOS COMMUNICATIONS CLUB THAN CHAOS COMPUTER CLUB. I DON'T

THINK YOU NEED THE COMPUTER. IT'S MORE FOR PEOPLE WHO THINK MORE THAN HACK, PERHAPS. THERE ARE ALSO HACKERS IN THE CLUB, SURE, THAT'S A BIT OF THE PROBLEM BECAUSE HACKERS HAVE DIFFERENT INTERESTS THAN PEOPLE LIKE US WHO ARE MORE INTERESTED IN COMMUNICATION AND ART. WHETHER THEY'RE JUST FREAKS THAT KNOW A LOT ABOUT THE TECHNICAL SIDE...

THERE ARE OTHER PEOPLE INTO REAL LIVE HACKING, LIKE SHOWING PRESS PASSES TO GET INTO THINGS, THAT'S REAL HACKING.

WHAT TYPE OF LAWS EXIST IN GERMANY TO DETER HACKING?

AT THE MOMENT WHEN YOU CHANGE SOMETHING IN SOMEONE ELSE'S COMPUTER, IT'S ALREADY AN OFFENSE. SO WHEN YOU LOGIN AND YOU'RE NOT SUPPOSED TO LOGIN, YOU CHANGE SOMETHING BECAUSE IT'S REPORTED SOMEWHERE THAT YOU HAVE LOGGED IN. SO YOU HAVE ALREADY CHANGED SOMETHING IF YOU FOLLOW THE LAW STRICTLY. I THINK THAT THEY ARE STILL WORKING ON THESE LAWS.

CALL OUR COMPUTER BULLETIN BOARDS!

CENTRAL OFFICE (914) 234-3260
YOYODYNE (402) 564-4518
BEEHIVE (703) 823-6591
HACKER'S DEN (718) 358-9209

All available 24 hours a day.

No registration necessary.

IF YOU'RE INTERESTED IN OPERATING A 2600 BBS, CONTACT US AT (516) 751-2600.

computer club

HAS ANYONE BEEN CAUGHT AND FINED ON A HACKING CHARGE?

THE ONLY THING THAT I CAN THINK OF IS STEVE IN PRISON, BUT HE HASN'T BEEN CHARGED.

CAN YOU GIVE ME SOME EXAMPLES OF MEDIA DISTORTION?

THERE WAS THIS BIT WITH A BANK IN HAMBURG, ON A VIDEOTEX SYSTEM IN GERMANY. IT HAS MANY MANY BUGS AND MANY MISTAKES IN IT AND WHEN YOU HAVE AN OVERFLOW OF DATA, ANYTHING COULD HAPPEN. SO IN THIS WAY THEY FOUND OUT THE PASSWORD OF THIS BANK IN HAMBURG AND THEY USED THIS, AND THEN THE CHAOS COMPUTER CLUB RAN A SECTION OF INFORMATION PAGES ON THE VIDEOTEX SYSTEM. THEY ALSO HAVE A MOVIE IN THERE WHICH YOU CAN LOOK AT BUT YOU HAVE TO GIVE A DONATION FOR LOOKING AT THE MOVIE -- FIVE DOLLARS, WHICH IS THE MAXIMUM SUM FOR LOOKING AT A VIDEOTEX PAGE.

Well, they made the bank look at this page over and over again. They wrote a little program so it was always calling it back again and had it run over the weekend so no one from the bank was there to stop it. In the end it was 150,000 MARKS WORTH OF DONATIONS FROM THE BANK TO THE CHAOS COMPUTER CLUB. THE CLUB COULD HAVE CLAIMED THE MONEY FROM THE BANK BECAUSE THERE ARE NO LAWS SAYING THAT THIS WASN'T OK. THEY DIDN'T, BUT THEY SHOWED THE NATIONAL DATA SECURITY OFFICE WHAT IS POSSIBLE. THE BANK WAS VERY THANKFUL FOR

THE HINT.

THE HOST OPERATOR OF THE SYSTEM SAID, "IT'S ONLY BECAUSE OF THE CHAOS COMPUTER CLUB THAT THE BETAX VIDEOTEX SYSTEM IS A FLOP." THEY WERE TELLING US AT THE DEMONSTRATION OF BETAX THAT IT WAS BECAUSE OF THE CHAOS COMPUTER CLUB THAT PEOPLE WON'T USE IT.

Also, whenever there is a show of the BETAX VIDEOTEX SYSTEM, people call up the club's movie on the demonstration accounts.

How does the phone system work in regard to modems? Is it digital or a clunking mechanical system?

YOU STILL HAVE THE CLUNK, CLUNK, CLUNK SYSTEM IN MOST TOWNS. THEY HAVE JUST STARTED TO CHANGE TO THE DIGITAL SYSTEM.

IF YOU WANT A MODEM YOU HAVE TO BUY IT OR RENT IT FROM THE POST OFFICE. OR YOU USE A HAYES MODEM WHICH IS ILLEGAL. THE MODEMS FROM THE POST OFFICE AREN'T VERY POWERFUL. THERE ISN'T ANY GOOD SOFTWARE TO WORK WITH THEM AND THEY'RE VERY EXPENSIVE. IN GERMANY IT IS FORBIDDEN TO DO ANYTHING YOURSELF WITH THE TELEPHONE LINE. THERE IS A JOKE THAT YOU EVEN NEED PERMISSION WHEN YOU USE A PEN TO DIAL THE PHONE.

IF YOU NEED A LONGER CABLE YOU HAVE TO GO TO THE POST OFFICE AND PAY 65 MARKS AND FILL OUT A REQUEST FORM FOR A LONGER CABLE TO YOUR TELEPHONE.

west germany's

SO PHONE PHREAKING IS NOT A HOT SUBJECT IN GERMANY?

THERE ARE SOMETIMES PEOPLE WHO TRY TO MAKE BLUE BOXES OR THINGS OF THESE KIND BUT I DON'T KNOW IF THEY WORK. THERE WAS ONE GUY WE KNEW WHO HAD A THING LIKE THIS, BUT HE DISAPPEARED INTO PRISON OR SOMEWHERE. WE HAVE TO TRY...MAYBE IT WILL WORK WHEN THE NEW SYSTEMS ARE INSTALLED. TELEPHONE CALLS ARE VERY EXPENSIVE IN GERMANY, ESPECIALLY LONG DISTANCE CALLS AND SO IT WOULD BE A USEFUL THING.

WE ARE CHARGED FOR ALL THE LOCAL CALLS IN UNITS OF EIGHT MINUTES IN THE DAY AND 12 MINUTES AT NIGHT.

WHAT HAPPENED TO STEFFEN WERRNEY WHEN HE WENT TO FRANCE?

STEFFEN WAS INVITED TO A SECURITY CONGRESS TO REPORT ABOUT WHAT HAPPENED WITH NASA AND TO EXPLAIN WHAT IS POSSIBLE IN THESE NETWORKS. HE WAS ARRESTED RIGHT AWAY WHEN HE ARRIVED AT THE AIRPORT IN FRANCE AND QUESTIONED FOR 24 HOURS. THEY KEPT HIM THERE WAITING WHILE THEY HAD ABSOLUTELY NO EVIDENCE WHATSOEVER THAT HE WAS IN ANY WAY INVOLVED IN THE NASA STORY.

WHAT ACTUALLY HAPPENED WITH NASA AS OPPOSED TO WHAT THE NEWSPAPERS SAID?

THEY'RE NOT MEMBERS OF THE CHAOS COMPUTER CLUB. THEY WERE ONE YEAR WORKING FOR A COMPANY AND SUDDENLY THEY

FOUND OUT THAT THEY WERE IN THE NASA NETWORK. AFTER A WHILE OF WORKING INSIDE THERE, THEY ONE DAY BEGAN TO UNDERSTAND THAT IT WAS VERY DANGEROUS.

THERE ARE STORIES ABOUT THE CIA -- THEY DON'T ASK QUESTIONS, BUT SHOOT FIRST. I DON'T BELIEVE THESE STORIES MYSELF, BUT THEN I THINK THE AMERICANS MUST BE SILLY...

THEN ONE DAY THEY PHONED AND CAME TO THE CHAOS COMPUTER CLUB AND SAID TO THE PEOPLE THERE, "WE HAVE SOME COMPUTER PRINTOUT AND WE DON'T WANT TO BE KILLED BY IT. WHAT SHALL WE DO?" STEFFEN AND WAU SAID OK, KEEP QUIET AND WE WILL USE OUR CONTACTS. THEN THE MACHINE STARTED. THEY TRIED TO GIVE INFORMATION TO THE CIA VIA THE GERMAN SECRET SERVICE. THEY SAW THAT ONE WEEK LATER THE ACCOUNT WAS STILL WORKING. THEY GAVE NOTICE TO THE COMPANY THAT WAS MANUFACTURING THE TERMINAL SOFTWARE. THEN THERE WAS A NEW VERSION DISTRIBUTED THAT STILL CARRIED THE SAME MISTAKE.

WHAT DID THE COMMUNICATION SOFTWARE ALLOW YOU TO DO?

IT ALLOWED YOU TO LOOK AT THE USER LIST. USUALLY IT TELLS YOU THAT YOU HAVE NO PERMISSION TO LOOK AT IT OR DO ANYTHING THERE. IT GAVE THE WARNING IN THE PROGRAM BUT IT WOULDN'T CUT YOU OFF. YOU COULD GO FARTHER DESPITE IT SAYING YOU COULDN'T.

SO THEY WENT IN AND GAVE THEMSELVES PRIVILEGES IN THE SYSTEM, AND THEY PUT IN THESE TROJAN HORSES -- PROGRAMS

"computer hackers"

THAT WIPED OUT ALL TRACES OF THEMSELVES IN THE SYSTEM SO NO ONE KNEW. IT ALSO COPIED ITSELF INTO OTHER SYSTEMS ON THE NETWORK AND BROUGHT BACK INFORMATION ABOUT PASSWORDS TO THE KIDS. THEY HAVE BEEN IN 135 DIFFERENT SYSTEMS.

Die HACKER Bibel I & II, WHAT IS IT?

YOU FIND SOME REPRINTS OF SOME AMERICAN STUFF IN IT (TAP), COMPLETE REPRINTS OF OLD DATENSCHAUER, AND SOME ARTICLES YOU WILL ONLY FIND IN THE BOOK. YOU CAN FIND THIS OVER THE COUNTER IN ANY BOOKSTORE.

I THINK IT HAS AN ISBN NUMBER. Die HACKER Bibel II is due soon. It's been printed. We're waiting for STEFFEN to send us copies. Die HACKER Bibel III is now being worked on.

258 pages softcover
ISBN 3-922708-98-6

Published by Der Grune,
Zweig 98, West Germany.

Cost 15 dollars US approximate.

- Original Material written for Bibel.
- Photocopy art/humour related to computers and hackers.

- News clippings and articles from various sources.

- Includes reprinted article about Hackers Conference.

- Reprints from Datenschauer.

- Early YIPL 1-22 reprints and TAP 23-27.

- About 40% of the book is in English.

- A good reason to learn German.

Chaos Computer Club:

D-2000, Hamburg 20 or

Schwenckestr. 85

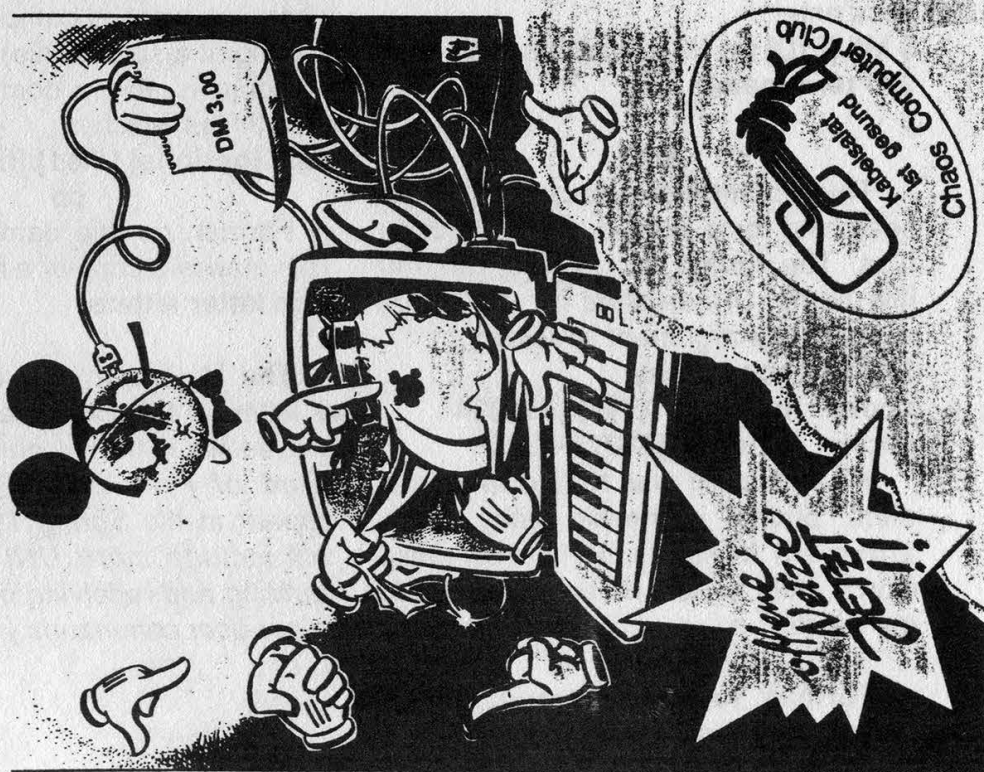
West Germany

01149404903757, 0114940483752.

Postverzeichnisschlüssel
037777
Nr. 21

Die Datenschleuder

Das wissenschaftliche Fachblatt für Datentechnik
Ein Organ des Chaos Computer Club



UNIX HACKING

(continued from page 17)

wd" command as shown below:

```
$passwd
Changing password for john
Old password:
New password:
Retype new password:
$
```

This will only work when the password has aged enough.

ps

It's sometimes necessary to see what command processes you are running. This command lets you see that. The format is: ps [-a all processes except group leaders] [-e all processes] [-f the whole list].

```
$ ps
```

```
PID TTY TIME COMMAND
```

```
200 tty09 14:20 ps
```

The system reports the PID - the process identification number which is a number from 1-30,000 assigned to UNIX processes. It also reports the TTY, TIME, and the COMMAND being executed at the time. To stop a process enter:

```
$ kill [PID] (in this case it's 200)
```

```
200 terminated
```

```
$
```

grep

This command is important when searching for a word or words in large files. The format is: grep [argument] [file name]. It searches for a file that contains the argument specified.

```
$ grep phone cathy
```

```
phone michelle (718)5551234
```

```
phone cindy (718)5553456
```

What this did was to find the argument "phone" in the file cathy. If the argument consists of two or more words, then it must be enclosed in single quotes.

mv

Format: mv [file names(s)] [dir name]. This renames a file or moves it

to another directory.

```
$ mv letter letters
```

```
$
```

This example renames the file letter to letters, thereby deleting letter. If you want to move files then you would enter:

```
$ mv /usr/john/pers/capital /usr/john/michelle/capital
```

```
$
```

This moves the file capital to the directory named michelle.

diff

Format: diff [file name] [file name]. This shows the difference between two files. Output of this will have something like 4,5c4,5 then it will display both sets of files on the screen. The 4,5c4,5 means that you must change "c" lines 4 to 5 in one file to line 4 to 5 in another.

Options for using this command are: -b (it ignores blank spaces), -h (compares it quickly), -s (reports files that are the same), -S[file] (this is used when you want to compare a directory starting at a specific file).

There is also a command to compare 3 files which is:

```
diff3 [options] [file1] [file2] [file3]
```

cp

Format: cp [file name] [file name].

This makes a copy of a file.

```
$ cp letter letters
```

```
$
```

The file letters is a duplicate copy of letter. In this case the original is not erased like in the mv command.

(End of Part One. Part Two will appear in the Spring 1989 issue and will include more UNIX commands, sending and receiving messages, and super user commands.)

2600 Marketplace

WANTED: Text files/ Countlegger/ Phrack news clippings on hackers, phreaks, etc. from newspapers and magazines. Willing to pay or trade. Send a list to KH, N. 11107 Roundup, Mead, WA 99021.

WANTED: Any hacking programs for the Atari ST. Will trade. Also in need of good blue box plans. Would love to hear from other persons interested in P/H from Lexington, KY. Aristotle, 606-258-2219.

COMPUTERIZED LEARNING USER'S GROUP, ELECTRONICS is for those interested in learning electronics and related technologies as well as those interested in developing, evaluating, sharing, and selling hardware and soft-

ware to do so. Write CLUGE, 207 East School Street, Kent, Ohio 44240-3837 or call 216-678-4611.

WANTED: Red box and/or blue box, tone chips for making boxes, Macintosh software for trade via mail or modem and vending machine lock-pick gun/tools. Douglas, PO Box 8022, Richmond, IN 47374.

FOR SALE: 3 Comtech model 550 Satellite Video Receivers. Best offer, first come, first served! Send reply to either dtroup@carroll1.uucp or send real mail to: DTROUP/Room 205st, 221 N. East Ave., Waukesha, WI, 53186. Skunk Works!

FOR SALE: Various UNIX manuals/books. For more information, write to Seth K., PO Box 245070, Brooklyn, NY 11224.

I WANT TO START a newsletter devoted to petty crimes, tentatively titled "For Informational Purposes Only". Please send me info, clippings, on how to rip-off vending machines, free postage, free photocopies, sneaking into movie theaters, etc. Tim Cridland, PO Box 85874, Seattle, WA 98145.

WILL TRADE: My Texas Instrument Silent 700 Series Portable Intelligent Data Terminal (like new) w/full documentation for any hacker software for IBM compatible computers. Ted K., PO Box 533, Auburn, NY 13021-0533.

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.

COMPLETE RANGE of Commodore 64 hack/phreak software. All tested and debugged. Many advanced applications. Call THC-J BBS at 604-595-0085

and leave feedback to the sysop for more information.

TAP BACK ISSUES, complete set Vol. 1-90 of QUALITY copies from originals. Includes schematics and indexes. \$100 postpaid via UPS or First Class Mail. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

2600 MEETINGS. First Friday of the month at the Citicorp Center—from 6 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info.

Deadline for Spring Marketplace: 3/1/89.

HARDWIRING

by Dr. Williams

One of the most obvious ways of obtaining free telephone service is through "hardwiring" -- that is, directly connecting a phone to somebody else's line without their knowledge. This can be accomplished in a few different manners. One technique is just to hook up a phone to the exterior of a house or business. Another way, canning, is a little less blunt. Any dime store phone can be hooked up, and wala! Free telephone service is yours just for the begging.

There are basically two types of exterior phone boxes that are used for homes and small businesses. The older ones are a pukey green color, are square, and have four terminals inside: two for the grounds, and two for the charged wires. These are kept closed by a long bolt. The newer ones are rectangular and have a phone jack inside of them. They are kept closed by a lid. There is only one tool you'll need, and that is a touch tone phone. The ones where all of the components are contained in the headset are the best for this. Take the cord, cut it in the middle, and strip the wires on both halves. There should be four wires: a green, red, black, and yellow. The green and red ones carry the current, and the black and yellow are the grounds. There could be some variations in the colors of the wires, depending on the phone, but there should always be two

grounds and two charged wires. After stripping the wires, put an alligator clip on the green and red wire on both halves. Putting one on the grounds is a good idea too.

Now you have what it takes to connect up to any phone box. On the older ones where there are just four terminal posts, you take the headset and connect up to the terminals via the alligator clips on the headset. You won't need to use the other half of the cord with the phone jack since there is no place to hook it up. You may also have to bring some vise grips to unscrew the bolt which holds the box closed. Sometimes, the colors of the terminals aren't marked, so it will take some trial and error to find the two live ones. On the newer boxes that have a telephone jack inside of them, you use the other half of your cord containing the jack to plug inside of it. Then you connect the alligator clips together on the headset. This should be no problem to open since they are held down with a plastic lid. Easy, isn't it! One note, though. There may be other variations out there. From my experience, these are the most common types of boxes.

There are some drawbacks; relationships are always two-sided. The good points are that it's easy (it beats hacking out codes to the local extender at the pay phone) and, since most residential areas still use AT&T as their pri-

YOUR WAY IN

mary carrier, you can call anywhere in the world. Some other long distance carriers have limited calling areas. The drawbacks are, first, you have to do this at night -- like, 3 or 4 am. If you do this, you always run the risk of getting caught. Some neighbor might think you're a prowler. You should therefore dress in dark clothes and not carry any identification with you. There is also a limited amount of things you can do. After all, you can't call up your relatives or too many of your friends at that time of day.

There is a wealth of locations where one can try to hook up. One spot is housing construction -- going up and coming down. Sometimes, when houses or apartments are being built, the phones are connected before construction is complete. I've also seen cases where people move out and the phones are not disconnected. Once the people lived in a mobile home and they moved out, leaving a vacant lot with a utility pole. Well, lo and behold, the phone was still connected. The phone company didn't disconnect it until about seven months later, and that was after practically everyone in the neighborhood had crank-called people in Japan and Australia. You can also try rural neighborhoods late at night, although using your own probably isn't a good idea.

Small business clusters or

industrial centers are also good spots. These usually have the green boxes clumped together in lots of four. Late at night, no one is around, so it's only a matter of hooking up. I'm talking about those places where a company leases the shop or office space to various companies. Trying to hook up where a 7-11 is located probably wouldn't be too smart.

Canning

A subject I'm going to touch upon is canning. The reason I say I just want to "touch" upon it is because this topic really deserves a whole article by itself, but since you can use the same tools of the trade, I'm going to mention it here. Cans are those ugly green containers that stick out of the ground. Most of the smaller and isolated cans can be easily opened with vise grips. The bigger ones sometimes have locks on them, but nothing a bolt cutter couldn't handle. Most cans that I've come across come in two flavors: ones where there are just masses of individual telephone wires clumped together, and the others that break apart the clumps of wires to help the distribution of the telephone wires. The ones that have just the bundles of wires clumped together I've found to be of little use. I imagine that a guy would have to match up the two wires for each single phone to get a current that will work. But then again, I'm not an expert.

HARDWIRING PHONE SERVICE

Sometimes these do break up a few individual houses in the neighborhood. There might be a metal plate attached to the top of the can with four or five terminals sticking out. Use trial and error again to find a live current. It is usually pretty easy. The other cans, the bigger ones which are sometimes locked, can be a goldmine. They usually distribute pairs of wires in a horizontal fashion, with a row of metal stubs sticking out. Inside it might look a bit confusing. Around the perimeter, there are wads of wires tangled together and going every which way. Inside the perimeter are rows and rows of square metallic stubs. These stubs are thin, about three eighths of an inch wide, and they stick out about an inch. The telephone wires will connect to both sides of the horizontal rows of these metallic stubs. All you need to do is connect up to two horizontal stubs. Not all of the wires in the can may be live, so you need more than one try. Sometimes these bigger cans have some goodies in them, such as lineman's headsets and papers containing technical data. From what I understand, the purpose of these cans is to help troubleshoot problems by breaking up units (or clusters of wires) into smaller units. I want to emphasize that I am not an expert on these cans. These are just my observations and I'm sure things work differently in different parts of the nation.

The real benefit of hooking up comes when you own a portable computer with a modem. If you find a target computer that you'd like to get to know better, and you're not stupid enough to try to get to it from your home phone, then this might be a good way to go. Portables are going down in price; I've seen some in pawn shops for about \$125.

There are a couple of other observations that I'd like to make. I've attended two different high schools and I found their long distance dialing procedures in the same place. On the principal's desk, there was a bread board that slid out on the left hand side. The instructions for making long distance calls were typed on a piece of paper taped to this location. Perhaps this is a common occurrence. I've also lived in a few different dorms, and I've noticed similarities in their setup too. In each room there was a plated telephone jack. The plate was only held down by two flathead screws. I unscrewed the plate and behind were most of the telephone wires for the whole floor. I could have hooked up to any room on the floor undetected.

Finally, if you find that any of the above works out pretty good for you, don't be too greedy, stupid, or start taking life for granted. As they say on Wall Street: "Bulls make money, bears make money, pigs get slaughtered."

BOOK REVIEW

Tune In On Telephone Calls

by Tom Kneitel

Published by CRB Research,
Box 56, Commack NY 11725

160 pages, \$12.95

Reviewed by Lou Scannon

Telephone calls have been carried on radio waves for years -- from ships at sea, from cars, and, since the advent of microwave and satellite technology, even the average long distance call travels through the ether for a portion of its route. And unlike the private medium of telephone wires, where a physical intrusion is required to listen in on the conversations, radio waves are everywhere around us and need only the right kind of receiver to pull them in.

Although most people know about the existence of car phones, there are a good number of other telephone services on the air: including cordless phones, local marine telephones, ships on the high seas and more. The conversations can range from the ordinary chitchat and gossip of your neighbors, to a lonely seaman talking to his wife or children, or to your local drug dealer planning his next purchase of controlled substances.

Alas, thanks to a recent act of Congress called the "Electronic Communications Privacy Act" (ECPA for short), listening to some kinds of telephone calls over the radio is illegal. Which kinds? Well, it's hard to say. If it's from a car,

then it's definitely illegal to eavesdrop, if it's from a cordless telephone, then it's maybe illegal, and if it's from a boat or airplane, then it's perfectly OK. The law does not specify how the radio enthusiast is supposed to be able to distinguish between protected traffic and unprotected traffic.

Fortunately, the Justice Department has announced that they have no plans to enforce this portion of the ECPA which is just as well, as the thought of the Feds breaking into your house to see where you have been tuning your radio tends to put a damper on radiotelephone eavesdropping.

From the editor of *Popular Communications* magazine comes a book that promises to explain how you can become a radio voyeur and listen in. And indeed it does, except by the time you come to the end of the book you're wondering what you paid for. More than a third of the book (60 pages) is composed of channel allocation charts of questionable value. There's no index or bibliography, the latter which would have been useful as the reader is referred to other books whenever the author declines to delve too deep into the technicalities. All in all, a steep price for a few frequency charts and a lot of folksy diatribe against the ECPA. Kneitel may have gotten too used to writing monthly magazine editorials and seems unable to talk about cellular

BOOK REVIEW: TUNE IN ON TELEPHONE CALLS

phones without sniping at the industry lobbyists and members of Congress who sponsored the ECPA. Although the ECPA is without a doubt bad legislation that fails to understand the technology it purports to regulate, Kneitel spends far too much space in an already sparse tome whining about it.

For the complete novice, there's a short chapter on what kind of equipment you'll need (a scanner that covers the 870-896 Mhz cellular band and a general coverage shortwave receiver), and a few tips on antennas. Kneitel has a few good words for the Radio Shack PRO-2004 scanner, which after a quick modification (also described in the book) becomes an efficient machine for following cellular calls.

The book covers each portion of the radio spectrum that contains something to do with telephone calls. Car phones, cordless phones, wilderness and remote area phones, radio common carriers, beepers, local marine, regional marine, high seas marine, and oil rigs.

Satellite and microwave links are briefly touched upon, but the equipment needed for intercepting microwave links isn't described. A little miscellany that might not be easily found elsewhere is also included, such as telephone company maintenance frequencies, experimental air and railroad phone services, and the MARS

military network used for patching phone calls for uniformed personnel on ships or at U.S. bases overseas.

Although the book is informative, it is a skinny volume at a fat price. With a little trimming, it would have made a good article in *Popular Communications*, and would only have cost \$2.50 at the newsstand. For more complete information on channel allocations, Radio Shack sells the "Police Call Radio Guide", which contains complete scanner frequency listings for a particular area. This will tell you just about everything, though it's in a hard to digest format and you'll have to dig for what you want. For station listings in the shortwave band, which will include a worldwide rundown of the maritime telephone frequencies and military MARS frequencies (but again they'll be buried among a lot of other frequency listings), see the "Confidential Frequency List", from Gilfer Shortwave (800-GILFER-1 or 201-391-7887, Box 239, 52 Park Avenue, Park Ridge, NJ 07656.

2600 meetings

**First Friday of the month in
the lobby of the Citicorp
Center, 53rd Street, between
3rd and Lexington, NYC from
5pm to 8pm. Call (516) 751-
2600 for more info.**

IMPORTANT NOTICE

Rising costs are forcing us to raise our subscription prices slightly. If you renew your subscription before March 1st, you can beat the increase. The old rates are to the left and the new ones are to the right. You can renew now even if your subscription doesn't expire for a long time. We'll just add the time on. You have the choice of tearing out this page and sending it back to us (your address label on the back tells us who you are) or sending one of your own pieces of paper explaining just what it is you want.

Please note that even though it obviously isn't the fourth quarter of 1988, this is the Winter 1988 edition and not the Spring 1989 one. We're sorry for any confusion.



INDIVIDUAL SUBSCRIPTION

- 1 year/\$15/\$18 2 years/\$28/\$33 3 years/\$41/\$48

CORPORATE SUBSCRIPTION

- 1 year/\$40/\$45 2 years/\$75/\$85 3 years/\$110/\$125

OVERSEAS SUBSCRIPTION

- 1 year, individual/\$25/\$30 1 year, corporate/\$55/\$65

LIFETIME SUBSCRIPTION

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

BACK ISSUES (never out of date and the same old price!)

- 1984/\$25 1985/\$25 1986/\$25 1987/\$25
 1988/\$25

TOTAL AMOUNT ENCLOSED:

CONTENTS

THE INTERNET WORM STORY	4
MCI RIPPING OFF CUSTOMERS	10
HACKER'S GUIDE TO UNIX	12
OVERHEARING PHONE CALLS	19
LETTERS	24
SOVIET OPERATORS	30
CHAOS COMPUTER CLUB	34
2600 MARKETPLACE	41
HARDWIRING FREE CALLS	42
REVIEW: TUNE IN ON PHONE CALLS	45

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

SECOND CLASS POSTAGE

Permit Pending at
East Setauket, N.Y.
11733

ISSN 0749-3851

WHERE WALS FOLGE
LÄSST DIE BALD

Forwarding and Address Correction Requested