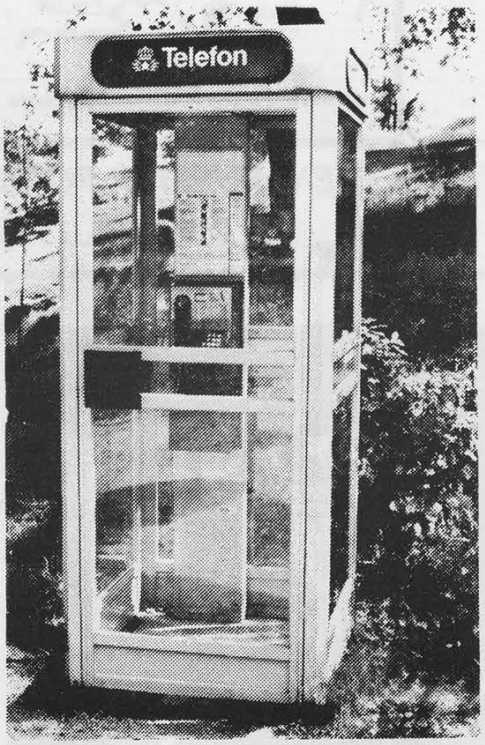
2600

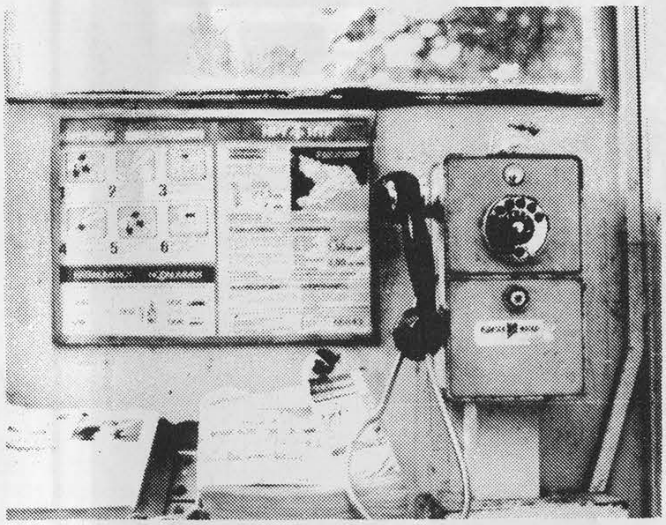
The Hacker Quarterly

VOLUME SEVEN, NUMBER FOUR
WINTER, 1990

SCANDINAVIAN PAYPHONES



A SWEDISH PAYPHONE AT DJVRGARDSBRON, STOCKHOLM



FINNISH PAYPHONE ON THE ISLAND FORTRESS OF SUOMENLINNA (SVEABORG), HELSINKI

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

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

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

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

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

STAFF

Editor-In-Chief
Emmanuel Goldstein / Alan Smithee

Artwork
Holly Kaufman Spruch

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

Remote Observations: Geo. C. Tilyou

Shout Outs: The subterranean chapter: Find the Power; dd: your Day will come, we promise; SS: thanks for making it interesting; Franklin; the few who have the strength to face the many; Screaming Target and the future; the millions held hostage.

a political

According to the *Philadelphia Inquirer,* a Republican staff member gained access to as many as 1,000 computer files and documents belonging to Democrats. The GOP staffer, Jeffrey Land, is reported to have admitted tapping into their files "many, many times" between July 1988 and the spring of 1990. Land was apparently able to gain access to files detailing "campaign contributions and the 1991 campaign strategy of the New Jersey Senate Democrats.

What's particularly appalling is that a secret legislative report indicates that his activities were known by his superiors who saw nothing wrong with what he was doing. "No one thought it appropriate to bring this fact to anyone's attention or deemed this to constitute an ethical breach," the report said.

A letter recently received by *2600* claims to reveal some inside information on this case. We'll let you be the judges.

I'd rather not divulge my real name, nor can I divulge my employers' names, not in light of an ongoing criminal investigation. Suffice it to say that I work for one of the two major political parties within the State of New Jersey and that, for the time being, I wish to maintain this job for a little while longer.

I report to the party leadership. I have been involved in politics for quite some time and now do a wide range of duties, among them issues of telecommunications security.

My telecommunications security skills, though hardly noteworthy in the presence of *2600's* readership, are somewhat respectable and tremendously aided by publications such as yours. This is why I wish to return a favor and contribute some of my insight for everybody's benefit.

Up front, I have been privy to much of what is going on in regards to the Jeffrey Land case.

Mr. Land was a former Assembly Aide to an Assemblyman, an assemblyman who, coincidentally, was among those implicated in the Pete Rose scandal (this assemblyman wrote a letter of recommendation on behalf of the guy who was indicted for participating in a cocaine ring selling to Rose).

"The Legislative Network is one system divided into sub-systems. It isn't too hard to get into one sub-system and out the other."

Land was smart. We were considered to be among the "bright boys".

Back in '88, we inadvertently broke through the user system of the WANG Legislative Network Systems and had found ourselves within the Systems Administrators' controls.

hacking scandal

I didn't stick around for too long. The only information I gained was a better understanding of how the system worked, but not the contents of the individual files stored within.

Land also busted through the users' system but didn't back out. He kept going on his own, all through '88, '89, and up to February of 1990 when he finally got caught.

The Land case is fascinating. It's been in the news around here for some time. Land had not only gotten into the system, but had also taken out interesting information, like contributor listings, campaign strategies, and such — all from the opposing political party.

The Legislative Network, you see, is one system divided into sub-systems. It isn't too hard to get into one sub-system and out the other. This is essentially what Land did.

Inquiries by the State Ethics Committee determined that the party leadership whom Land was working for was not only aware of this, but "saw nothing wrong in what he was doing."

Incredible. What's even more fascinating is that the opposing political party whose files have been exposed are not seeking to press any charges and wish to instead "forget about the whole thing." This, despite the acknowledged fact that Land managed to see and/or obtained well over 1,000 individually protected files!

Why back down?

Here's why.

Land uncovered solid, hard evidence including:

1) State staff, hired solely for the benefit of service to the public were working solely for the benefit of the elected officials on public money and time using public facilities, notably computer databasing facilities and the like. Public tax money for state staff salaries was therefore used to keep elected officials in office. Everybody does this, *but it's not supposed to be known outside of the office.*

2) Land's computer evidence directly correlates between given contributions and posted legislation. The major stumbling block for election-law overseers is that you cannot readily tell who is being given what. PAC (Political Action Committee) money is handed out in such a way that election law reports do not readily tell who actually benefits from these contributions. PAC's are deliberate fronts for corporations and others who do not want to leave a trail. Land obtained evidence showing what corporation gained what piece of legislation — tax breaks, funding loopholes, etc. — in a manner never done before.

"How can we reasonably expect our legislators to legislate on our behalf on such crucial telecommunications matters when they are, in fact, among those breaking the law?"

More Weirdness

Election-law controls are obviously

a hacking

in need of expansion. In light of what happened in the fall of '89, the Land case underlines this point. During October of '89, the current majority leadership members were implicated in a so-called "shake-down" of a lawyer's PAC. Among the so-called statements said to the lawyer's PAC representatives during that fateful dinner meeting was the now famous line: "Your members are going to be upset if your bills don't get posted." The FBI and the Attorney General's office later exonerated them of the allegations, but a bad taste still lingers.

We've all known about this shit; corruption is as old as the human race. A politician taking money — so what else is new? The catch is how can we reasonably expect our legislators to legislate on our behalf on such crucial telecommunications matters when they are, in fact, among those breaking the law? *Our legislators are among those encouraging partisan hacking!*

"It's not how you play the game, it's whether you win. Winning is, after all, everything."

I recall vividly what our director for our legislative staff said to me: "It's not how you play the game, it's whether you win. Winning is, after all, everything."

Great.

It is utterly ironic that, when approached upon the issue of "hackers" and the like, legislators crank out their "total distaste toward these individuals" while all along whatever information hackers cull they greedily accept, seeing "no apparent ethical wrongdoing" as Land's superiors so stated.

The State Attorney General's office announced that they "see no need to further investigate the matter." The Speaker of the House said that "the public doesn't give a tinker's damn about the situation." The argument flowing to the newspapers about the "fundamental separation of powers between the legislative and the executive branch of government" is garbage. The separation argument is, actually, a means of ducking the real issue: election funding reform. Ironically, both partisan political parties, Republican and Democrat, do agree upon avoiding this one issue as next year's elections are looming on the horizon.

I write this because you state in your article on "Operation Sundevil" that we should write to our legislators. Actually, as one who works closely with legislators, they really don't "give a tinker's damn", unless, of course, you're a large, multi-national PAC. After helping to set up the fundraisers, I've watched the legislative bills get posted and know *there's no such thing as coincidence at the state capital.*

I, for my part, feel that this country is rapidly becoming a tremendously twisted nightmare; it's one thing to have soldiers goosestepping down

political scandal

Pennsylvania Avenue, but something else when we're living within a giant David Lynch sitcom.

It is time that we start politicizing ourselves. (*Ha!* A hacker's PAC, anyone?!) It's time to start working together before more shit comes down the pike. Expect to see regulations, BBS licensing, and the like to come about, all in the name of raising taxes for these "tough economic times". Taxation and operational regulations are what the Secret Service and the legislators want, both as a means of a "better regulatory/law enforcement" and for raising more money to channel into other programs or job perks for relatives on the payrolls.

"The computer expert is becoming the samurai of these petty lords."

Never mind, though, that most of the boards would go under due to lack of sufficient funds to keep them going. This scenario also doesn't mention that those remaining BBS's would do so only by charging or increasing their operational charges. Our cutting edge gets dull and us with it — unless, of course, you've become a member of The New Movement, the Underground Net.

It's Getting Cold Around Here

Several other trends are becoming evident: the winnowing of Freedom of Information Act file acquisitions (see June of '90 American Bar Association Magazine), the lack of accountability on the part of credit bureaus obtaining private information from branches of the U.S. government (isn't it an amazing coincidence that TRW, the credit bureau, is also TRW, the major defense industry corporation?), and now the crackdown on BBS's — yep, surf's up: the stormtide's rising, gang.

The Lords of Disorder

Watergate lives on. I was recently hired by a congressperson on their campaign telecommunications/-databasing system. Somebody broke into this congressperson's system and got a listing of the major databases. No disks were stolen or damaged, not that anything ever is, and the office doors were, interestingly enough, not forced open. After an "inter-office investigation", custodial staff was found to have been "lax" and, although not proven, it appears that it was a primary election candidate's worker who managed to get in and check out the files.

This was bad. Once you know when, where, who, and what voting block your opponent is gunning, well, then you're fucked. Political strategy must then be shifted accordingly, and this can be a real pain in the ass.

This last story and the Land case illustrates how the computer expert is becoming the samurai of these petty lords, particularly those experts who stand on "the edge". Perhaps herein lies our true strength.

We are far stronger than what we're given to be; this is why the SS is strong-arming us and why corrupt politicians employ our skills while yet taxing our life's blood.

THE HACKER

by Dr. Williams

This article lists sources of computer security information of interest to hackers. The list is divided into six parts: underground magazines, catalogs, books, journals, newsletters, and network mailing lists. Each is given a brief description and information is provided on obtaining the product. This list is not intended to be comprehensive.

The information presented on the profiled magazines is up to date for the most part; a few sources are up to 18 months old. Therefore, before sending money, confirm the address and subscription rate by contacting the company. Some companies will send sample issues if asked.

Subscription rates denoted by "*freebie" indicates the magazine is free to qualified people. To become a qualified person, contact the company and tell them of your desire to receive their magazine. They will send a confirmation card asking some questions, including your company and job title. Good occupational choices are System Consultant or System Administrator.

Underground Magazines

TAP. After several revival attempts by various groups after the original, one of them managed to succeed. Written with the same flavor as the old *TAP,* but does not pick up where the old *TAP* left off. The anarchist-technical voice is there, but the chaotic shoe-string budget effect and loud voice is missing. Published whenever they have material to create an issue. Subscription rates are $10 a year, ($15 for Canada, $20 for overseas). Address: TAP, P.O. Box 20264, Louisville, KY, 40250.

Processed World. The magazine with the bad attitude towards technology. An analytically oriented, office centered magazine about work. Specifically its concerns are the drawback of work in a technological society with their "Tales of Toil" from around the area. $12 for 4 issues. Address: 41 Sutter St. #1829, San Francisco, CA 94104.

Fractal Report. A newsletter for those reasonably skilled in programming who wish to explore computer images of the Madelbrot set and its relatives. It's a shame they don't have color printing, but even the monochrome screen dumps here are rather interesting. Languages used include C, Pascal, and Forth. $23 for six issues. Address: J. de Rivax, c/o Fractal Reeves Telecommunications, West Town House, Porthtowan, Cornwall, TR4 8AX, United Kingdom.

The Capital District Computer Mart. A local magazine available by mail. In addition to the ads from area computer stores, they've got reviews and feature articles. Information useful to everyone is in every issue. $2 for four issues. Address: P.O. Box 402, Schenectady, NY 12301.

The Amateur Computerist. This forum grew out of a programming class for workers at Ford. It's sort of an experiment in bringing computing ideas to the shop floor grassroots. Mostly it's history and short programs in basic. Hasn't really taken off yet, but the potential is there. $5 for four issues. Address: R. Hauben, P.O. Box 4344, Dearborn, MI 48126.

Puget Sound Computer User. A local newspaper from the Seattle area with widespread appeal. Most articles cover topics of concern to everyone. Only the ads and events are local. $12 a year. Address: Puget Sound Computer User, 3530 Bagely Ave. N., Seattle, WA 98103, phone 206-547-4950.

Full Disclosure. A magazine for citizens interested in knowing and exercising their rights to the maximum legal extent. Emphasis placed on knowing rights against legally empowered authorities. $24 for twelve issues, published irregularly. Address: Full Disclosure, P.O. Box 8275, Ann Arbor, Michigan, 48107.

Cybertek. A better than usual survival/technological magazine. Computer anti-security mixed in with surveillance and survival. $15 for a year, $20 overseas. Published six times a year. Address: Cybertek Magazine, P.O. Box 64, Brewster, NY 10509.

Intertek. "The Cyberpunk Journal". A new publication on high tech. Single issues are $2.50, a year's subscription is $7. Address: Intertek, 325 Ellwood Beach, #3, Goleta, CA 93117. Make checks out to Steve Steinberg.

Hack-Tic. Holland's answer to 2600. $24 by international money order. Address: Hack-Tic, P.O. Box 22953, 1100 DL, Amsterdam, The Netherlands.

Catalogs of Books

Loompanics Unlimited. Self proclaimed publishers and sellers of unusual books, and they're right. Their catalog deals with most every subject. Areas the books are classified by: the underground economy, making money, tax evasion, privacy and hiding things, fake ID, big brother is watching, conducting investigations, crime and police science, frauds and con games, computer crime, locks and locksmithing, ninja, self defense, revenge, guns, silencers, knives, bombs and explosives, guerrilla warfare, murder and torture, survival, head for the hills, self sufficiency, gimme shelter, health and life extension, paralegal skills, sex, drugs, and rock and roll, intelligence increase, science and technology, heresy/weird ideas, anarchism and egoism, reality creation, and self-publishing. $2.50 for a catalog of books. Address: Loompanics Unlimited, P.O. Box 1197, Port Townsend, WA 98368.

Consumertronics. Like the Loompanics catalog, except more focused on technology and more aggressive, if that's possible. Sometimes they're successful, sometimes not. Information published in newsletter format, not books. As a result, less information is covered, but what is there is hard-

READING LIST

packed; a "how to" style is presented. Areas covered: computers, energy theft, phones, rip-offs, survival, and other technology and governmental agencies issues. $1.00 for a catalog. Address: Consumertronics, 2011 Crescent Dr., P.O. Box Drawer 537, Alamogordo, NM 88310.

CRB Research Books, Inc. Biggest selection of books describing all sorts of wireless communication: scanning frequencies, eavesdropping, jamming, CB's, shortwaves, radio directories, etc., plus the usual assortment of books dealing with underground technology, with a mishmash of other interesting books. $1.00 for a catalog. Address: CRB Research Books, Inc., P.O. Box 56, Commack, New York 11725.

FactSheet Five. The best, and only, complete source of underground magazines currently published — magazines which have anywhere from one to thousands of subscribers. Lists and reviews most current underground magazines in a catalog-type format. Contains a good number of magazines that are published outside the United States as well. Editor Mike Gunderloy does an excellent job describing and evaluating each "fanzine" in a paragraph. His reviews are objective, pointing out both good and bad features. These objective reviews are accurate most every time.

Most of the underground fanzines available can be plugged into one of these categories: political, poetry, musical, sports, anarchy, science fiction, entertainment, philosophy, religious, comics, current topics, sub-culture, sex, special interest, and various rantings and ramblings. *Factsheet Five* reviews pamphlets, books, and audio as well. $3.00 per issue. Address: Mike Gunderloy, 6 Arizona Avenue, Rensselaer NY 12144-4502. 24-hour answering machine (518) 479-3707. 300/1200/2400 baud computer bulletin board (518) 479-3879.

Catalogs of Products

Advanced Electronic Technologies. Product categories available: non-lethal weapons, transmitter detectors, telephone recorders, telephone tap detectors, parabolic microphones, microwave detectors, "infinity" security devices, video camera detectors, telephone privacy modules, subcarrier detectors, infra-red viewers, specialty microphones, audio jammers, tracking systems, telephone controllers, bullet-proof vests, gun hideaways, gas masks, chemical light sticks, countermeasure systems, specialty publications, and video surveillance equipment. $3.00 for a catalog. Address: Advanced Electronic Technologies, Suite 173, 5800-A N. Sharon Amity Rd., Charlotte, N.C., 28215.

Sherwood Communications Associates LTD. Product categories available: investigative aids, stealth, communications, video, van equipment, microphones, tape recorders, telephone accessories, telco tools, telephone recorders, monitoring, countermeasures, books, videos, and training materials. Address: Sherwood Communications Associates LTD, 1310 Industrial Highway, Southhampton, PA 18966. Phone: (215) 357-9065.

Gall's Inc. A catalog of products primarily for police and firemen: lightbars, gun and equipment holders, traffic movers, security items, traffic control, vehicle accessories, scanners, radios, antennas, flashlights, books, and handcuffs. Address: Gall's, P.O. Box 55268, 2470 Palumbo Dr., Lexington, KY 40555-5268. Phone: 800-524-4255. Fax: 606-269-4360.

Selective Books

Hackers. By Steven Levy. The history of hackers from 1960-1984 as heroes of the computer revolution. A dynamic book: well written, thoroughly interesting, and completely researched. Sometimes a bit hokey in making his "Hacker's Ethic" fit the circumstances, but overall a must read.

The Hacker's Handbook. By Hugo Cornwall. The first book specifically written for computer hackers. An excellent overall book, but technically lightweight when it comes to actually discussing hacking. ISBN 0-912579-06-4. Published by E. Arthur Brown Company; phone 612-762-8847.

Out of the Inner Circle. By Bill Landreth (now in its second edition). Bill Landreth was a member of a highly competent group of hackers before hacking became the latest rage. He was caught, convicted, sentenced, and lived to tell about it all in his book. ISBN 0-914845-36-5. Published by Microsoft Press.

The Computer Underground. By M. Harry. 20% good, 80% bad. Half the book contains old text files which have been around forever on the BBS circuit and are now obsolete. The book has its bright spots and chooses its subjects well, but is overall written poorly. Especially irritating is his incorrect analysis of mathematical chance and probabilities. ISBN 0-915179-31-8. Published by Loompanics Unlimited.

Die Hacker Bibel I & II. A bit of everything from the Chaos Computer club: some original material, news clipping, old *TAP* articles, Hackers Conference material, and computer art/humor. Over half of the material is written in German. ISBN 3-922708-98-6. Published by Der Grune. Also available through the Chaos Computer Club, Schwenckestr 85, D-2000 Hamburg 20, Germany.

The FBI and Your BBS. A guide for sysop's worried about legal security. 75% is fluff, 25% is the information the sysop needs to know. Published by The FBI Project. Phone (313) 747-7027.

The Cuckoo's Egg. By Clifford Stoll. This book has been in the news so much, any comments here would only by repetitious. ISBN 0-385-24946-2. Published by Doubleday.

Viruses

Computer Viruses, a High-Tech Disease. By Ralf

Burger. Bill Machrine, editor of *PC Magazine* described this book best: "...I've just seen what may be the most ill-conceived computer book ever. I can't bring myself to tell you the title, author, or publisher. This book about viruses strikes me as the height of opportunistic publishing and bad judgement.... Instead of a book offering a way to protect yourself against viruses...this is a how-to manual.... I knew this book had gone beyond the pale when I got to the chapters on attacking hardware, which included techniques for destroying monitors and disk drives...." ISBN 1-55755-043-3. Published by Abacus.

Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System. By John McAfee, Chairman of the Computer Virus Industry Association. A good book by someone who knows what viruses are. Covers all aspects of viruses: history, human factors, and computer considerations. Includes code for the more famous viruses. ISBN 0-312-03064-9. Published by St. Martin's Press.

Other worthy books mentioned briefly:

Computer Related Crime. All aspects superficially covered. Available from Loompanics.

Turing's Man. By J. David Botler.

Soul of a New Machine. By Tracy Kidder.

Neuromancer, Count Zero, Mona Lisa Overdrive, and *Burning Chrome.* All by William Gibson.

Unix System Security. By Robert Morris Senior. One of the best books on Unix security.

Computer Lib, 1987 Edition. By Ted Nelson. A counterculture computer book.

Computer Security Sources

(The majority of this list appeared in Computer Security Information Sources, by Russell Kay, *Computer Security Journal,* Volume IV, Number 1, pages 29-40.)

Computer Security Journal. Covers most topics as they relate to computer security, including software, hardware, and human factors. Published two times a year. $65 for a year ($60 for CSI members), 96 pages long. Address: Computer Security Institute, 360 Church Street, Northborough, MA 01532, phone (617) 393-2600.

Computers & Security. Aimed at the academic and technical oriented people. Published six times a year. $131.05 for a year. Address: Elsevier Journal Information Service, 52 Vanderbilt Avenue, New York NY 10017, phone (212) 916-1250.

Computer Security, Audit, and Control. Mostly brief digests of articles which have appeared in other magazines or newsletters, though it does contain some original material. Published 2 times a year. $55 for a year, around 60 pages per issue. Address: Management Advisory Publications, P.O. Box 151, Wellesley Hills, MA 02181, phone (617) 235-2895.

Data Processing & Communications Security. Covers a broad range of computer security subjects. Published four times a year. $30 for a year, 40 pages long. Address: Assets Protection, P.O. Box 5323, Madison, WI 53705, phone (608) 231-3817.

Internal Auditor. Discusses techniques of internal control and auditing. Published two times a month. $24 a year for non-members, free for members. Address: Institute of Internal Auditors, 249 Maitland Avenue, Altamonte Springs, FL 32701, phone (305) 830-7600.

Security (formerly *Security World*). For the loss prevention conscious person working in industrial or commercial areas. Published once a month. *freebie. Address: P.O. Box 5510, Denver, CO 80217, phone (303) 388-4511.

Security Management. For the manager in charge of security and preventing losses. Published once a month. $30 for a year, or included with an annual membership to the American Society for Industrial Security, it's $65 for the first time and then $55 to renew. Address: ASIS, 1655 N. Fort Meyer Drive, Suite 1200, Arlington, VA 22209, phone (703) 522-5800.

Security Systems Administration. For the person in charge of security, going over a wide range of topics, including retail. Published once a month. *freebie. Address: PTN Publishing Company, 201 Crossways Park Drive, Woodbury, NY 11797, phone (516) 496-8000.

Contingency Journal. The magazine for business planning. *freebie. Address: 10935 Estate Lane, Suite 375, Dallas, TX 75238, phone (214) 343-3717.

Telecommunications. Not about computers, but about telephones and network technology. Mentioned here because it's a *freebie. Address: 685 Canton Street, Norwood, MA 02062, phone (617) 769-9750.

Newsletters

Computer Crime Digest. Provides information relating to computer fraud and crimes. Published 12 times a year. $136 for a subscription, 10-12 pages long. Address: Washington Crime News Services, 7043 Wimsatt Rd, Springfield, VA 22151, phone (703) 941-6600.

Computer Fraud & Security Bulletin. Reports computer crime and how to prevent it. $240 for a subscription, 12 pages long. Address: Elsevier Journal Information Center, 52 Vanderbilt Ave., New York, NY 10164, phone (212) 916-1250.

Computer Law Newsletter. Covers all aspects of computer law and crime. Published twice a month. *freebie. Address: Warner & Stackpole, 28 State Street, Boston, MA 02109, phone (617) 951-9000.

Computer Security Newsletter. Discusses a wide range of subjects for the person in charge and responsible for computer security. Published twice a month. You must have a membership with the Computer Security Institute, $95 per year domestic, or $125 for overseas. 8 pages long. Address: Computer Security Institute, 360 Church Street, Northborough, MA 01532, phone (617) 393-2600.

HACKER LITERATURE

Computer Security Products Reports. Reviews computer security products. Published 4 times a year. $16 for a subscription. Address: Assets Protection, P.O. Box 5323, Madison, WI 53705, phone (608) 231-3817.

Computer/Law Journal. Discusses issues relating to computer law. Published quarterly. $76 for a year by the Center for Computer/Law, 112 Ocean Drive, Manhattan Beach, CA 90266.

Personal Identification News. For advanced access control technologies and practices, covering most devices and techniques. Published 11 times a year. $265 per year. Address: *Personal Identification News,* P.O. Box 11018, Washington DC, phone (202) 364-8586.

Privacy Journal. Reports all issues on personal privacy as affected by technology. Published monthly, 8 pages long. $89 for a year. Address: P.O. Box 15300, Washington, DC 20003, phone (202) 547-2865.

Security Letter. Their thrust is towards commercial and industrial security, stressing commercial security planning and physical security systems. Published twice a month. $137 for a year. Address: *Security Letter,* 166 East 96th Street, New York, NY 10128, phone (212) 348-1553.

Security Systems Digest. Keeps the reader up to date on the most recent developments in security systems for the commercial and industrial security practitioner. Published two times a week. $120 for a year, 10-12 pages. Address: Washington Crime News Services, 7043 Wimsatt Road, Springfield, WA 22151, phone (703) 941-6600.

Network Mailing Lists. To subscribe to a mailing list, send a message including your name and network address. There are over 250 mailing lists available covering a wage ranges of topics through the networks.

CERT. The Computer Emergency Response Team mailing list covering the latest virus attacks, discovered security holes, and appropriate patches. CERT.SEI.CUM.EDU

Computer Underground Digest. The best news available concerning the underground computer community. Covers most topics of interest to hackers. TK0JUT2@NIU.bitnet

ETHICS-L. Discussion of computer ethics. Usually generates more heat than light. Bitnet subscribers issue command: SUBSCRIBE ETHICS-L (your full name) to: LISTSERV @MARIST.BITNET

Other subscribers may write to: JROBINET%POLYTECH.BITNET@CUNYVM.CUNY.EDU

Fanzine. An electronic monthly science fiction magazine. fanzine %PLACI.SUN.COM

INFO-MODEMS. A discussion group of special interest to modem users. Info-Modems-Request@SIMTEL20.ARPA

INFO-UNIX. A question/answer forum for novice users, programmers, and administrators of the Unix operating system. INFO-UNIX-REQUEST@BRL.ARPA

INFO-VAX. Not to be outdone, the VMS operating system has its own forum for questions and answers. INFO-VAX-REQUEST@KL.SRI.COM

List of mailing lists. The current "list of lists" of mailing groups available. ZELLICH@SRI-NIC.ARPA

PACKET-RADIO. A discussion where people can exchange ideas about packet radio and discuss current projects. PACKET-RADIO-REQUESTS @EDDIE.MIT.EDU

RISKS. Distribution list for discussion of issues related to risks to the public in the use of computer systems. Sponsored by the ACM. RISKS-REQUEST@CSL.SRI.COM

SECURITY. Discusses all types of security. Most of the focus is on computers and locks of all sorts. SECURITY-REQUEST@AIM.RUTGERS.EDU

SF-LOVERS. A forum for science fiction fans of all topics. Bitnet subscribers issue the command: TELL LISTSERV at RUTMV1 SUBSCRIBE SFLOVERS (your full name). All others write to SF-LOVERS-REQUEST@RUTGERS.EDU

TELECOM. The best forum of all telephone related topics. Get this and your mailbox will never be empty again! eecs.new.edu!telecom

Archives of telecom are available at lcs.mit.edu in the telecom-archives directory.

UNIX-WIZARDS. For people maintaining machines running the Unix operating system. UNIX-WIZARDS-REQUEST@BRL.ARPA

VIRUS-L. Forum specifically for the discussion of all topics of computer viruses. Bitnet subscribers issue the command: SUB VIRUS-L (your full name).

Other subscribers include the same command in the message body to: LISTSERV%LEHIIBM1.BITNET @MITVMA.MIT.EDU

2600 has meetings in New York and San Francisco on the first Friday of every month from 5 pm to 8 pm local time. See page 41 for specific details.

CLIP AND DISCARD

Central Office

This is one of the last articles to come out of The Legion of Doom
by Agent Steal

I should point out that the information in this article is correct to the best of my knowledge. I'm sure there are going to be people that disagree with me on some of it, particularly the references to tracing. However, I have been involved in telecommunications and computers for 12+ years.

I'm basing this article around the 1AESS since it is the most common switch in use.

Outside Plant

This is the wiring between your telephone and the central office. That is another article in itself so if you are interested read Phucked Agent 04's article on outside loop in the *LOD Technical Journal*. It explains those green boxes you see on street corners, aerial cables, manholes, etc. Where it stops, this article starts.

Cable Vault

All of the cables from other offices and from subscribers enter the central office underground. They enter into a room called the cable vault. This is a room generally in the basement located at one end or another of the building. The width of the room varies but runs the entire length of the building. Outside cables appear though holes in the wall. The cables then run up through holes in the ceiling to the frame room.

Understand that these cables consist of an average of 3600 pairs of wires. That's 3600 telephone line. The amount of cables obviously depends on the size of the office. All cables — interoffice, local lines, fiber optic, coaxial — enter through the cable vault.

Frame Room

The frame is where the cable separates to individual pairs and attaches to connectors. The frame runs the length of the building, from floor to ceiling. There are two sides to the frame, the horizontal side and the vertical side. The vertical side is where the outside wiring attaches and the protector fuses reside. The horizontal side is where the connectors to the switching system reside. Multi-conductor cables run from the connectors to actual switching equipment. So what we have is a large frame called the Main Distribution Frame (MDF) running the entire length of the building, floor to ceiling 5 feet thick. The MDF consists of two sides, the VDF and the HDF. Cables from outside connect on one side and cables from the switching equipment connect to the other. Jumper wires connect the two. This way any piece of equipment can be connected to any incoming "cable pair". These jumper wires are simply 2 conductor twisted pair running between the VDF and HDF.

What does all this mean? Well, if you had access to COSMOS you would see information regarding cable and pair and "OE" or originating equipment. With this you could find your line on the frame and on the switch. The VDF side is clearly marked by cable and pair at the top of the frame, however the HDF side is a little more complicated and varies in format from frame to frame and from one switch to another. Since I am writing this article around the 1AESS, I will describe the OE format used for that switch.

OE ABB-CDD-EFF where: A = Control group (when more than one switch exists in that C.O.); B = LN Line Link Network; C = LS Line Switching Frame; D = CONC or concentrator; E = Switch (individual, not the big one); F = Level. There is one more frame designation called LOC or location. This gives the location of the connector block on the HDF side.

Switching Systems

Writing an article that covers them all would be lengthy indeed. So I am only going to list the major ones and a brief description of each.

Step by Step (Strowger 1889). First automatic, required no operators for local

calls, no custom calling or touch tone, manufactured by many different companies in different versions, hard wire routing instructions, could not chose an alternate route if programmed route was busy. Each dial pulse tripped a "stepper" type relay to find its path.

No. 1 Crossbar (1930); - No. 5 Crossbar (1947) (faster, more capacity). Western Electric, first ability to find idle trunks for call routing, no custom calling or equal access, utilized a 10x20 cross point relay switches, hard wired common control logic for program control, also copied by other manufacturers.

No. 4 Crossbar. Used as a toll switch for AT&T's long line network, 4-wire tandem switching, not usually used for local loop switching.

No. 1ESS (1966); - No. 1AESS (1973). Western Electric, described in detail later in file.

No. 1EAX. GTE Automatic Electric, GTE's version of the 1AEES, slower and louder.

No. 2ESS (1967); - No. 2BESS (1974). Western Electric, analog switching under digital control, very similar to the No. 1ESS and No. 1AESS, downsized for smaller applications.

No. 3ESS. Western Electric, analog switching under digital control, even smaller version of No. 1AESS, rural applications up to 4500 lines.

No. 2EAX. GTE Automatic Electric, smaller version of 1EAX, analog switch under digital control.

No. 4ESS. Western Electric, toll switch, 4-wire tandem, digital switching, uses the 1AESS processor.

No. 3EAX. Gee, is there a pattern here? No, GTE. Digital toll switch, 4-wire tandem switching.

No. 5ESS. AT&T Network Systems, full scale computerized digital switching, ISDN compatibility, utilizes time sharing technology, toll or end office.

DMS 100 Digital Matrix Switch. Northern Telecom, similar to 5ESS, runs slower, considerably less expensive.

DMS 200. Toll and Access Tandem, optional operator services.

DMS 250. Toll switch designed for common carriers.

DMS 300. Toll switch for international gateways.

No. 5EAX. GTE Automatic Electric, same as 5ESS.

How much does a switch cost? A fully equipped 5ESS for a 40,000 subscriber end office can cost well over 3 million dollars. Now you know why your phone bill is so much. Well... maybe your parent's bill.

The 1ESS and 1AESS

This was the first switch of its type placed into widespread use by Bell. Primarily an analog switch under digital control, the switch is no longer being manufactured. The 1ESS has been replaced by the 5ESS and other full scale digital switches. However, it is still by far the most common switch used in today's class 5 end offices.

The #1 and 1A use a crosspoint switching matrix similar to the crossbar. The primary switch used in the matrix is the fereed (remreed in the 1A). It is a two-state magnetic alloy switch. It is basically a magnetic switch that does not require voltage to stay in its present position. Voltage is only required to change the state of the switch.

The #1 utilized a computer style common control and memory. Memory used by the #1 changed with technology, but most have been upgraded to RAM. Line scanners monitor the status of customer lines, crosspoint switches, and all internal, outgoing, and incoming trunks, reporting their status to the central control. The central control then either calls upon program or call store memories to choose which crosspoints to activate for processing the call. The crosspoint matrixes are controlled via central pulse distributors which in turn are controlled by the central control via data buses. All of the scanners, AMA tape controllers, pulse distributors, x-

point matrix, etc., listen to data buses for their address and command or report their information on the buses. The buses are merely cables connecting the different units to the central control.

The 1E was quickly replaced by the 1A due to advances in technology. So 1A's are more common. Also, many of the 1E's have been upgraded to 1A's. This meant changing the fereed to the remreed relay, adding additional peripheral component controllers (to free up central controller load) and implementation of the 1A processor. The 1A processor replaced older style electronics with integrated circuits. Both switches operate similarly. The primary differences were speed and capacity. The #1ESS could process 110,000 calls per hour and serve 128,000,000 lines.

Most of the major common control elements are either fully or partially duplicated to ensure reliability. Systems run simultaneously and are checked against each other for errors. When a problem occurs the system will doublecheck, reroute, or switch over to auxiliary to continue system operation. Alarms are also reported to the maintenance console and are in turn printed out on a printer near the control console.

Operation of the switch is done through the Master Control Center (MCC) panel and/or a terminal. Remote operation is also done through input/output channels. These channels have different functions and therefore receive different types of output messages and have different abilities as far as what type of commands they are allowed to issue. Here is a list of the commonly used TTY channels.

Maintenance: Primary channels for testing, enable, disable, etc.

Recent Change: Changes in class of service, calling features, etc.

Administrative: Traffic information and control.

Supplementary: Traffic information supplied to automatic network control.

SCC Maint: Switching control centers interface.

Plant Service Center: Reports testing information to test facilities.

At the end of this article you will find a list of the most frequently seen Maintenance channel output messages and a brief description of their meanings. You will also find a list of frequently used input messages.

There are other channels as well as backups but the only ones to be concerned with are Recent Change and SCC Maint. These are the two channels you will most likely want to get access to. The Maintenance channel doesn't leave the C.O. and is used by switch engineers as the primary way of controlling the switch. During off hours and weekends the control of the switch is transferred to the SCC.

The SCC is a centrally located bureau that has up to 16 switches reporting to it via their SCC maint. channel. The SCC has a mini-computer running SCCS that watches the output of all these switches for trouble conditions that require immediate attention. The SCC personnel then has the ability to input messages to that particular switch to try and correct the problem. If necessary, someone will be dispatched to the C.O. to correct the problem. I should also mention that the SCC mini has dialups and access to SCCS means access to all of the switches connected to it.

The Recent Change channels also connect to a centrally located bureau referred to as RCMAC. These bureaus are responsible for activating lines, changing class of service, etc. RCMAC has been automated to a large degree by computer systems that log into COSMOS and look for pending orders. COSMOS is basically an order placement and record keeping system for central office equipment, but you should know that already, right? So this system called MIZAR logs into COSMOS, pulls orders requiring recent change work, then in one batch several times a day, transmits the orders to the appropriate

Central Office Tick

switch via its Recent Change Channel.

Testing of the switch is done by many different methods. Bell Labs has developed a number of systems, many accomplishing the same functions. I will only attempt to cover the ones I know fairly well.

The primary testing system consists of the trunk test panels located at the switch itself. There are three and they all pretty much do the same thing: test trunk and line paths through the switch.

Trunk and Line Test Panel
Supplementary Trunk Test Panel
Manual Trunk Test Panel

MLT Mechanized Loop Testing is another popular one. This system, often available through the LMOS database, can give very specific measurements of line levels and losses. The "TV Mask" is also popular giving the user the ability to monitor lines via a call back number.

DAMT Direct Access Mechanized Testing is used by line repairman to put tone on numbers to help them find lines. This was previously done by Frame personnel, so this automated that task. DAMT can also monitor lines, however the audio is scrambled in a manner that allows one only to tell what type of signal is present on the line, or whether it is busy or not.

All of these testing systems have one thing in common. They access the line through a "No Test Trunk". This is a relay (in the 1ESS) which can drop in on a specific path or line and connect it to the testing device. The test trunks are part of the switch itself and act like a telephone line into the switch. The function of this line is strictly for access and testing of subscriber lines. It depends on the device connected to the trunk, but there is usually a noticeable click heard on the tested line when the No Test Trunk drops in. Also the testing devices I have mentioned here will seize the line, busying it out. This will present problems when trying to monitor calls — you would need to drop in on calls in progress. The No Test Trunk is also the method in which operator consoles do verifications and interrupts.

Interoffice Signalling

Calls coming into and leaving the switch are routed via trunks. The switches select which trunk will route the call most effectively and then retransmits the dialed number to the distant switch. There are several different ways this is done. The two most common are Loop Signaling and CCIS, Common Channel Interoffice Signaling. The predecessor to both of these is the famous and almost extinct "SF Signaling". This utilized the presence of 2600 hz to indicate trunk in use. If one winks 2600 hz down one of these trunks, the distant switch would think you hung up. Remove the 2600, and you have control of the trunk and you could then MF your own number. This worked great for years. Assuming you had dialed a toll-free number to begin with, there was no billing generated at all. The 1AESS does have a program called SIGI that looks for any 2600 winks after the original connection of a toll call. It then proceeds to record on AMA and output any MF digits received. However due to many long distant carriers using signaling that can generate these messages it is often overlooked and "SIG IRR" output messages are quite common.

Loop signaling still uses MF to transmit the called number to the distant switch. However, the polarity of the voltage on the trunk is reversed to indicate trunk use.

CCIS, sometimes referred to as CCS#6, uses a separate data link sending packets of data containing information regarding outgoing calls. The distant switch monitors the information and connects the correct trunk to the correct path. This is a faster and more efficient way of call processing and is being implemented all over. The protocol that AT&T uses is CCS7 and is currently being accepted as the industry standard. CCS6 and CCS7 are somewhat similar.

Interoffice trunks are multiplexed together onto one pair. The standard is 24

(continued on page 18)

ATTACHMENT 1

"CLASSIFICATIONS"

Definitions and Examples of Discourteous Actions Which Warrant Discipline:

1. NOT BUSINESSLIKE:

Definition: Not exhibiting tone and manner felt to be appropriate in business - e.g., talking in a joking or jesting manner at inappropriate times. Use of slang - non-standard vocabulary.

Example: Customer: "I would like to call person to person the Sales Manager."

Operator: "Got ya." "Does he have a name and gimme the number."

or

"Oh, calling a big shot today."

2. RUDE, ANTAGONISTIC, ABUSIVE:

Definition: Offensive in manner or action. Ill-mannered, abrupt, forceful, argumentative, impatient, sarcastic, cutting. To provoke hostility, abuse verbally.

Example: Customer: "Operator, did you say the Area Code was 213 or 212?"

Operator: "The trouble with you is you don't listen." "I'll tell you once more 2-1-2 and don't ask again."

or

"Can't you understand English?" "I said 2-1-2!"

Example: Customer: "When am I going to get my number, Operator?"

Operator: "Never if I had any say about it." "If you weren't so dumb you could dial it yourself."

or

"When I feel like it." "Don't rush me."

3. SWEARING, VULGAR:

A. Profane:

Definition: To use profanity. To debase by wrong, unworthy or vulgar statements. Irreverent.

Customer: "Hey, operator where have you been out to coffee?" "I'm ready for another call."

Operator: "Just one damn minute." "Who the hell do you think you are, someone special?" "Anyway it's none of your G.D. business."

or

"Customers like you give me a pain - you know where."

B. Obscene:

Definition: Disgusting, repulsive, dirty, foul, nasty, vile, unprintable.

Example: Customer: "You connected me with a wrong number, now try it again."

Operator: "Oh, sh--, customers like you frost my a--."

or

"Tough, kiss my a--."

The above examples are intended to be the mildest description of each category.

THIS COMES FROM AN UNNAMED PHONE COMPANY'S MANUAL FOR SUPERVISORS. DOESN'T IT JUST FROST YOUR A--?

(continued from page 15)

channels per pair. This is called T-1 in its analog format and D-1 in its digital format. This is often referred to as carrier or CXR. The terms frame error and phase jitter are part of this technology which is often a world in itself. This type of transmission is effective for only a few miles on twisted pair. It is often common to see interoffice repeaters in manholes or special huts. Repeaters can also be found within C.O.'s, amplifying trunks between offices. This equipment is usually handled by the "carrier" room, often on another floor. Carrier also handles special circuits, private lines, and foreign exchange circuits.

After a call reaches a Toll Switch, the transmit and receive paths of the calling and called party are separated and transmitted on separate channels. This allows better transmission results and allows more calls to be placed on any given trunk. This is referred to as 4 wire switching. This also explains why during a call, one person can hear crosstalk and the other can't. Crosstalk is bleed-over from other channels on the multiplexed T-Carrier transmission lines used between switches.

Call Tracing

So with loop signaling standard format there is no information being transmitted regarding the calling number between switches. This therefore causes the call tracing routine to be at least a two-step method. This is assuming you are trying to trace an anticipated call, not one in progress. When call trace "CLID" is placed on a number, a message is output every time someone calls that number. The message shows up on most of the ESS output channels and gives information regarding the time and the number of the incoming trunk group. If the call came from within that office, then the calling number is printed in the message. Once the trunk group is known, it can usually be determined what C.O. the calls are coming from. This is also assuming that the calls are coming from within that Bell company and not through a long distance carrier (IEC). So if Bell knows what C.O. the calls are coming from, they simply put the called number on the C.I. list of that C.O. Anytime anyone in that C.O. calls the number in question another message is generated showing all the pertinent information.

Now if this were a real time trace, it would only require the assistance of the SCC and a few commands sent to the appropriate switches (i.e. NET-LINE). This would give them the path and trunk group numbers of the call in progress. Naturally the more things the call is going through, the more people will need to be involved in the trace. There seems to be a common misconception about the ability to trace a call through some of the larger packet networks like Telenet. Well, I can assure you, Telenet can track a call through their network in seconds and all that is needed is the cooperation of the Bell companies. Call tracing in itself is not that difficult these days. What is difficult is getting the different organizations together to cooperate. You have to be doing something relatively serious to warrant tracing in most cases, however, not always. So if tracing is a concern, I would recommend using as many different companies at one time as you think is necessary, especially US Sprint. They can't even bill people on time much less trace a call.

Equal Access

The first thing you need to understand is that every IEC (Inter Exchange Carrier) — or long distance company — needs to have an agreement with every LEC (Local Exchange Carrier) — or your local phone company — that they want to have access to and from. They have to pay the LEC for the type of service they receive and the amount of trunks, and trunk use. The cost is high and the market is a zoo. The LECs have the following options.

Feature Group A: This was the first access form offered to the IECs by the LECs. Basically whenever you access an IEC by dialing a regular 7 digit number (POTS line), this is FGA. The IEC's

equipment would answer the line, interpret your digits, and route your call over their own network. Then they would pick up an outgoing telephone line in the city you were calling and dial your number locally. Basically a dial in, dial out situation similar to PC Pursuit.

Feature Group B: FGB is 950-xxxx. This is a very different setup from FGA. When you dial 950, your local switch routes the call to the closest Access Tandem (Toll Switch) in your area. There the IECs have direct trunks connected between the AT and their equipment. These trunks usually use a form of multiplexing like T-1 carrier with wink start (2600hz). On the incoming side, calls coming in from the IEC are basically connected the same way. The IEC MFs into the AT and the AT then connects the calls. There are a lot of different ways FGB is technically set up, but this is the most common.

Tracing on 950 calls has been an area of controversy and I would like to clear it up. The answer is yes, it is possible. But like I mentioned earlier, it would take considerable manpower which equals expensive to do this. It also really depends on how the IEC interface is set up. Many IECs have trunks going directly to class 5 end offices. So, if you are using a small IEC, and they figure out what C.O. you are calling from, it wouldn't be out of the question to put CLID on the 950 number. This is highly unlikely and I have not heard from reliable sources of it ever being done. Remember, CLID generates a message every time a call is placed to that number. Excessive call trace messages can crash a switch. However, I should mention that brute force hacking of 950s is easily detected and relatively easy to trace. If the IEC is really having a problem in a particular area, they will pursue it.

Feature Group C: FGC is reserved for and used exclusively by AT&T.

Feature Group D: FGD is similar to FGB with the exception that ANI is MFed to the IEC. The end office switch must have Equal Access capability in order to transmit the ANI. Anything above a crossbar can have it. I guess I should mention that it is possible for a crossbar to have it with modifications. FGD can only be implemented on 800 numbers and if an IEC wants it, they have to buy the whole prefix. You should also be aware that long distance companies offer a service where they will transmit the ANI to the customer as well. You will find this being used as a security or marketing tool by an increasing amount of companies. A good example would be 800-999-CHAT.

1AESS Common Output Messages

(Message is followed by a description.)

Alarm

AR01: Office alarm
AR02: Alarm retired or transferred
AR03: Fuse blown
AR04: Unknown alarm scan point activated
AR05: Commercial power failure
AR06: Switchroom alarm via alarm grid
AR07: Power plant alarm
AR08: Alarm circuit battery loss
AR09: AMA bus fuse blown
AR10: Alarm configuration has been changed (retired, inhibited)
AR11: Power converter trouble
AR13: Carrier group alarm
AR15: Hourly report on building and power alarms

Automatic Trunk Test

AT01: Results of trunk test

Carrier Group

CG01: Carrier group in alarm
CG03: Reason for above

Coin Phone

CN02: List of pay phones with coin disposal problems
CN03: Possible Trouble
CN04: Phone taken out of restored service because of possible coin fraud

Copy

COPY: Data copied from one address to another

Call Trace

CT01: Manually requested trace line to line, information follows

CT02: Manually requested trace line to trunk, information follows
CT03: Intraoffice called placed to a number with CLID
CT04: Interoffice called placed to a number with CLID
CT05: Call placed to number on the CI list
CT06: Contents of the CI list
CT07: ACD related trace
CT08: ACD related trace
CT09: ACD related trace

Digital Carrier Trunk

DCT COUNTS: Count of T carrier errors

Memory Diagnostics

DGN: Memory failure in cs/ps diagnostic program

Digital Carrier "Frame" Errors

FM01: DCT alarm activated or retired
FM02: Possible failure of entire bank, not just frame
FM03: Error rate of specified digroup
FM04: Digroup out of frame more than indicated
FM05: Operation or release of the loop terminal relay
FM06: Result of digroup circuit diagnostics
FM07: Carrier group alarm status of specific group
FM08: Carrier group alarm count for digroup
FM09: Hourly report of carrier group alarms
FM10: Public switched digital capacity failure
FM11: PUC counts of carrier group errors

Maintenance

MA02: Status requested, print out of MACII scratch pad
MA03: Hourly report of system circuits and units in trouble
MA04: Reports condition of system
MA05: Maintenance interrupt count for last hour
MA06: Scanners, network, and signal distributors in trouble
MA07: Successful switch of duplicated unit (program store etc.)
MA08: Excessive error rate of named unit
MA09: Power should not be removed from named unit
MA10: OK to remove paper
MA11: Power manually removed from unit
MA12: Power restored to unit
MA13: Indicates central control active
MA15: Hourly report of number of times interrupt recovery program acted
MA17: Centrex data link power removed
MA21: Reports action taken on MAC-REX command
MA23: 4 min. report, emerg. action phase triggers are inhibited

Memory

MN02: List of circuits in trouble in memory

Network Trouble

NT01: Network frame unable to switch off line after fault detection
NT02: Network path trouble Trunk to Line
NT03: Network path trouble Line to Line
NT04: Network path trouble Trunk to Trunk
NT06: Hourly report of network frames made busy
NT10: Network path failed to restore

Operating System Status

OP:APS-0
OP:APSTATUS
OP:CHAN
OP:CISRC: Source of critical alarm, automatic every 15 minutes
OP:CSSTATUS: Call store status
OP:DUSTATUS: Data unit status
OP:ERAPDATA: Error analysis database output
OP:INHINT: Hourly report of inhibited devices
OP:LIBSTAT: List of active library programs
OP:OOSUNITS: Units out of service
OP:PSSTATUS: Program store status

Plant Measurements

PM01: Daily report
PM02: Monthly report
PM03: Response to a request for a specific section of report
PM04: Daily summary of IC/IEC irregularities

Report

REPT:ADS FUNCTION: Reports that an ADS function is about to occur
REPT:ADS FUNCTION DUPLEX FAILED:

# of a Central Office

No ADS assigned
REPT:ADS FUNCTION SIMPLEX: Only one tape drive is assigned
REPT:ADS FUNCTION STATE CHANGE: Change in state of ADS
REPT:ADS PROCEDURAL ERROR: You fucked up
REPT:LINE TRBL: Too many permanent off hooks, may indicate bad cable
REPT:PROG CONT OFF-NORMAL: System programs that are off or on
REPT:RC CENSUS: Hourly report on recent changes
REPT:RC SOURCE: Recent change system status (RCS=1 means RC Chan. inhibited)

Recent Change

RC18: RC message response

Remove

RMV: Removed from service

Restore

RST: Restored to service status

Ringing and Tone Plant

RT04: Status of monitors

Software Audit

SA01: Call store memory audit results
SA03: Call store memory audit results

Signal Irregularity

SIG IRR: Blue box detection
SIG IRR INHIBITED: Detector off
SIG IRR TRAF: Half hour report of traffic data

Traffic Condition

TC15: Reports overall traffic condition
TL02: Reason test position test was denied
TL03: Same as above

Trunk Network

TN01: Trunk diagnostic found trouble
TN02: Dial tone delay alarm failure
TN04: Trunk diag request from test panel
TN05: Trunk test procedural report or denials
TN06: Trunk stat change
TN07: Response to a trunk type and status request
TN08: Failed incoming or outgoing call
TN09: Network relay failures
TN10: Response to TRK-LIST input, usually a request from test position
TN11: Hourly, status of trunk undergoing tests
TN16: Daily summary of precut trunk groups

Traffic Overload Condition

TOC01: Serious traffic condition
TOC02: Reports status of less serious overload conditions

Translation (shows class of service, calling features, etc.)

TR01: Translation information, response to VFY-DN
TR03: Translation information, response to VFY-LEN
TR75: Translation information, response to VF:DNSVY
TW02: Dump of octal contents of memory

1AESS Common Input Messages

Messages always terminate with ". ctrl d ", x=number or trunk network #

NET-LINE-xxxxxxx0000: Trace of path through switch
NET-TNN-xxxxxx: Same as above for trunk trace
T-DN-MBxxxxxxx: Makes a # busy
TR-DEACTT-26xxxxxxx: Deactivates call forwarding
VFY-DNxxxxxxx: Displays class of service, calling features etc.
VFY-LENxxxxxxxx: Same as above for OE
VFY-LIST-09 xxxxxxx: Displays speed calling 8 list

***

There are many things I didn't cover in this article and many of the things I covered, I did so very briefly. My intention was to write an article that explains the big picture, how everything fits together. I hope I helped.

Special thanks to all the stupid people, for without them some of us wouldn't be so smart and might have to work for a living. Also special thanks to John and Dave for without their guidance, this would have never been written. Yes, people, there are great hackers out there that no one has ever heard of. You just have to know where to find them.

anatomy of

In our last issue, you may have noticed a reference to a service called 1-900-STOPPER on pages 25-26 that allows you to place a call without being Caller-ID'd for $2 a minute. We referred to it as "another rip-off that preys on people's fears." We also said it didn't allow you to call 800 numbers which frequently identify the numbers of their callers.

It looks like we ruffled some feathers. The following letter was sent to us by Will Dwyer, President and CEO of Private Lines, Inc. and a copy sent to their lawyer, M.L. Rudnick:

"Having gained knowledge yesterday of your having published in the Autumn 1990 issue of *2600 Magazine* (pages 25-26) that our telephone service, which you characterize as 'another rip-off,' 'won't allow you to call 800 numbers,' we hereby (1) serve notice on you of our claim that your statement is libelous and (2) demand that it be corrected. (Section 48a, Civil Code of California.)

"Had you either inquired of us or tried the service yourself, you would have found that a caller can reach an 800 number — without transmitting ANI (automatic number identification) for his or her phone number — via the same procedure by which our 1-900-STOPPER (786-7737) service allows call completion to any other U.S. telephone number. (Your writer, 'EH,' should have noted that the $2 per minute applies to calls anywhere in the U.S., not 'just local.' The $5 per minute service is a separate one for international calls; access to it is via 1-900-RUN WELL (786-9355)."

In a typical issue of *2600,* we point out quite a few discrepancies, inequities, or rip-offs. In each case we have specific knowledge which leads us to our conclusions. In this particular instance, we were replying to a letter ("EH" wrote the letter and is not one of our writers). We believed at the time, and we still do, that our assessment was correct.

This attempt to intimidate us into taking back our words does nothing but infuriate us. We have an obligation to be honest and open with our readers and no one person, company, or governmental agency will convince us to betray or suppress that trust.

Let's take a closer look at 1-900-STOPPER. We first tried calling 800 numbers through their service months ago. It didn't work. It still doesn't. We challenge anyone to use this service to make an 800 call to MCI (800-444-4444) or the Runaway Hotline (800-999-9999) or *any* 800 number. We did finally find one that worked, (AT&T: 800-222-0300). But the majority we tried didn't. We got a fast busy signal indicating some kind of a restriction.

Out of fairness, we cannot say that the service doesn't connect to 800 numbers. It does, sometimes. But one thing the service did do consistently was bill us for every attempt we made. Which brings us to the word "rip-off". A service that bills customers for absolutely nothing is, in our opinion, a very good example of this. If you use 1-

a rip-off

900-STOPPER to connect to a number that's busy, you'll still get billed $2 for the attempt.

Even if the system worked perfectly and only billed for the actual time connected, we still find its premise absurd. $2 a minute to make a local call or toll-free call? (There would be little need to use the service to dial nationally since there is currently no form of caller identification in place for long distance calls. Caller ID is only used locally and ANI is only used on toll-free calls, at least for the moment. It's true that there would be no long distance phone bill linked to the caller but if he/she were under surveillance, the digits they dialed would still show up on a pen register.)

As for this other service (1-900-RUN WELL), we find $5 a minute an obscene amount to charge for a phone call to anywhere. And what kind of privacy is being guaranteed here? Any international call is still subject to monitoring by the NSA. Your phone could still be tapped. A pen register could still be on your line. There is no international Caller ID or ANI to avoid.

We tried this service as well and found it disturbing. There was no mention at all of the high price. (Perhaps this helps explain why our letter writer got the pricing wrong.) All we were told was to enter the international number we wanted to call. We got a recording from AT&T saying all circuits were busy as well as a sinking feeling that we were going to get charged $5 for the privilege of hearing that bit of information.

Do we have anything at all good to say about these two services? Yes. It's good to recognize the right to privacy and let people know they don't have to be constantly monitored. There should always be alternatives to that. But, for the reasons given, we find these particular alternatives to be wholly inadequate ones.

Itemized calls, continued

Directly dialed

No.	Date	Place called	Number called	Time	Rate	Min.	Amount
		UK	4481	5 14 PM	DD	28	20.32
		NETHERLAND	3120	5 44 PM	DD	1	1.35
		MULTIQUEST	900 786-7737	4 51 AM		1	2.00
		MULTIQUEST	900 786-7737	4 40 PM		1	2.00
		MULTIQUEST	900 786-7737	4 41 PM		1	2.00
		MULTIQUEST	900 786-7737	4 42 PM		1	2.00
		MULTIQUEST	900 786-7737	4 43 PM		2	4.00
		MULTIQUEST	900 786-7737	4 45 PM		1	2.00
		NETHERLAND	3120	1 16 PM	DD	3	2.95
		SAUDI ARAB	9663	5 32 PM	DD	3	4.11
		GER FED RP	4930	2 16 PM	DD	1	1.42

Only the last attempt resulted in a successful call completion. But that didn't stop these wonderful people from billing us anyway.

IT'S THE

COCOT Troubles

Dear 2600:

I am presently enrolled in a senior high school in Fayetteville, NC. This school is robbing its students blind by having two COCOTs in the lobby. I obtained a copy of *2600* through a friend and I am interested in receiving more. Furthermore, I would like to request some extra information in hacking out these COCOTs so that I can get free LD's. My friend noted that these phones used a hangup pulse that hung up the phone when it read zero volts on the line. So he hooked in a nine volt battery in parallel until the number connected. I want to see if there are other less difficult ways of hacking this phone.

KM

By all means figure out how the phone works, but if all you're interested in is making free phone calls, you're not a whole lot better than the sleazoids who installed the phone in the first place. See what happens after the called party hangs up. Do you by chance get an unrestricted dial tone on your end? Look for speed dials that are programmed in via the star or pound keys. And see what happens when you call it. We suggest reading The Plague's COCOT article (Summer 1990).

Future Surveillance

Dear 2600:

The article "New Revelations from BellSouth" (by Emmanuel Goldstein, Autumn 1990) describes new monitoring technology. From this description, it appears to be a well-designed system for performing such monitoring. The author appears to believe that BellSouth should have improved their security in a different way.

However, wasn't the goal of some of the attacks against various Bell computers to demonstrate that Bell should improve their security? Why, then, the objection when they actually do so? And shouldn't they be free to select the method that they use?

fin
Minnesota

Not when that method carries extremely troubling implications. Note that the monitoring device BellSouth is interested in is capable of far more than "improving security". It can watch a variety of lines simultaneously, recording voice, fax, and computer transmissions automatically. Its configuration leads one to the conclusion that any interested entity will be able to monitor an individual thoroughly, even without the phone company's knowledge or approval. That's something none of us will be served by.

Why Did You Do It?

Dear 2600:

I was disappointed to see that you published the credit card algorithm in your Fall 1990 issue.

Although I know it was well within your First Amendment rights to publish it, I think that it serves no purpose by being published except to leave innocent credit card holders open to abuse by individuals who just wish to call a phone sex line or place a long distance call over an AOS. And although I know that the algorithm was already well known within the hacker world, I don't believe that your magazine should have spread it further.

In previous issues of *2600*, you stated that credit card fraud and long distance code abuse are tantamount to stealing and have nothing to do with the hacker ethic of learning and exploring systems. Therefore, I see no reason to publish the credit card algorithm if your magazine truly believes in the above. The only uses of the credit card algorithm by your readers would be to generate numbers to be used to place calls over an AOS, access to phone sex lines or 800 chat lines which use credit card numbers for billing, or to obtain actual merchandise as the authors of your article state that often credit card numbers are often checked only against the algorithm and then billed later.

Please stick to your ideals. If you believe that credit card fraud and code abuse are stealing and not hacking, then please do not publish any information that would be used to those ends. And please try not to publish materials from authors who call themselves names such as "K00l/RaD Alliance!". Your mag will end up looking like a "s00per-elYte c0dez phile!".

Questmaster
Santa Barbara, CA

You raise good points, but you've missed the point of 2600. We published that information so people would understand how the technology worked. What they do with that information is not our business. Read on

LETTERS PAGE

for another opinion.

Dear 2600:

In the article "An Algorithm For Credit Cards", there was an error in the C code that caused the program to incorrectly determine the weighting factor for 13 digit Visa cards. Here is a correct version, as employed in the form of a function:

```
is_valid_cc(kind, card_number)
int kind;
char *card_number;
{
  char ccn[30];
  int validP = 0;
  int cclen = 0, llen = 0;
  int cdigit = 0, csum = 0;

    cclen = strlen(strncpy(&ccn,
card_number, 30));

  /* is this the right length for this
kind of card? */
  switch(kind) {
  case VISA:
    if (((cclen != 13) && (cclen != 16)) ||
(ccn[0] != '4'))
      return(0);
    break;
  case MC:
    if ((cclen != 16) || (ccn[0] != '5'))
      return(0);
    break;
  case AMEX:
    if ((cclen != 15) || (ccn[0] != '3'))
      return(0);
    break;
  default:
    return(0);
  }

  for (llen=0; llen < cclen; llen++) {
    cdigit = ccn[llen] - '0';
    if ((llen + 1) % 2) cdigit *= 2;
    if (cdigit >= 10) cdigit -= 9;
    csum += cdigit;
  }
  if ((csum % 10) == 0) return(1);
  return(0);
}
```

This function will return 0 if incorrect, 1 if correct. "VISA", "MC" and "AMEX" are arbitrarily defined constants, and may be ignored.

Thank you for including this article — we have needed something to keep people from 'fumble-fingering' on card entries.

Kenton A. Hoover
Chief Engineer
Whole Earth Lectronic Link

Questions

Dear 2600:

I very much enjoy your magazine and I am curious whether certain companies tell the federal government or the phone companies the names of people that send away for crystals to make a red box.

Also, please print the frequencies of each touch tone. I'm writing melodies with them.

Rob
Woodmere, NY

It's not beyond the realm of possibility that some companies do that. The solution is to do what appeals to you and not worry about what others think, whether they be ignorant people or malignant bureaucracies. Touch tones are comprised of two frequencies each. Picture your touch tone keypad, with the extra A-B-C-D column on the right. Then place the following frequencies along the top: 1209 hz, 1336 hz, 1477 hz, and 1633 hz. From top to bottom the frequencies are: 697 hz, 770 hz, 852 hz, and 941 hz. Find the number you want and combine the two tones for that number and you've got a touch tone!

BBS Troubles

Dear 2600:

I have recently read the two articles about the E911 case that were published in the Spring 1990 edition of your magazine. First of all, I want to thank you for bringing things like these into the open. The federal government is always trying to keep their misconduct (which occurs all too often) under their hats, and it's great to see that people still have the guts to stand up to it.

I have also been feeling the effects of these "crackdowns" here in the Twin Cities. Many a BBS have disappeared (along with their operators). Many more have been looked into, but allowed to remain. Almost every BBS in the state now posts a warning message about the "privacy" of e-mail. I feel sorry for one BBS in particular: Hotline. It was clearly known to everyone that this BBS was completely legitimate. Yet, recently, they were the subject of a federal investigation. Apparently they had a set of users that were referred to as "privileged users". Someone who was uninformed and didn't take the

time to look into things further assumed that the "privileged users" were hackers and received access to some secret part of the BBS. Actually, a "privileged user" is someone who contributes money to the BBS and receives privileges such as more online time, extra downloads, etc. The operators have since changed the status to "contributors" rather than "privileged users" to avoid future confusion. It is hard to believe that this anti-hacker paranoia has grown to such proportions that people even get harassed for merely contributing money to a BBS that they like. In any case, I'm glad to see that this board, as well as many others, has survived the attacks and has the pride, determination, caring, and guts to remain in operation.

Finally, since my interest in cases such as these has grown recently, I would like to know what else is going on. Here in the Twin Cities, I have been waging a battle of my own: against censorship. I am concerned about how successful the PMRC (Parent Music Resource Center) has been in limiting the rights of musicians to say what they feel. Also, I feel that hackers are not doing anything that would cause harm to anyone, and should also be guaranteed the right to the First Amendment. I would like to receive more information about your magazine and how I may subscribe to it. I want to assure you that I am not a federal agent, nor do I have any contacts with the federal government. I am not interested in busting you or your magazine, but simply in learning more about what is going on.

The Spectre
St. Paul, MN

It wouldn't matter if you were. We provide the same information to anyone who's interested. We hope to see hacker bulletin boards recover from what has been a crippling blow. There are a great deal that are truly underground now. The need for public hacker boards has never been greater. Anyone who has questions about this should contact us.

Dear 2600:

I have been hearing rumors that the Federal Communications Commission is going to begin forcing BBS sysops to keep printed logs of their BBS's up to three years back. As a BBS sysop, I find it good practice to keep my logs, but after all of the work I've put into the board, I don't want the government telling me what I should do with it!

Charlie Tuna
Kokomo, IN

This is only one of the many pressures being put on system operators. Another is the threat of charging business phone rates to bulletin boards, an action that would put many of them out of existence. Counter these threats by uniting with your users and other system operators. And by sending letters to major publications like us.

Another Method

Dear 2600:

I just received your Autumn 1990 issue and, like always, I read it cover to cover. Very enjoyable and entertaining. I am involved with modifying scanners to get cellular, reprogramming cellular phones (for the obvious reasons), data reception from satellites, and just about anything else that is beyond the normal grasp. I have the programming procedure for over 45 cellular phones and a complete listing of tower codes for all states, several COCOT payphone manuals, and wiring diagrams. Between your magazine and the URR Newsletter, I get lots of ideas. For your readers that don't know, URR Newsletter sells lots of unusual parts and plans. I have been a fan of theirs for years. I got my start in CBs and progressed from there. Just thought I would let you know that I appreciate your existence.

Now for the good stuff. Recently I found a COCOT that had the serial numbers on the lock mechanisms. It don't get any easier than that. After opening the phone I discovered a programming switch inside. Now I can remove the static ram to dump the passwords and, to my delight, I now have an operating payphone. Just for fun, I left it in the same location, with the passwords changed of course. I'm really not into theft. I just like to explore. Bin 99 holds the programming access code, default is 99. Bin 96 holds the accounting access code. Default is, you guessed it, 96. You would be surprised to know how many phones are still in default. Ain't it wonderful? Using the ANI number supplied by *2600* will yield any COCOT number that is not on the outside of the phone. Call the phone and enter 99. If you gain access, it's fun to play around. ##0 will reset all bins to default (except

password, time, and date). ##10 will reset the rate table bins to 0. ##11 will enter the rate table adjustment mode. Bin 11 is the rate for local calls and Bin 12 controls the Intra-Lata (1+ seven digits) calls. Bin 14 controls the long distance calls. Naturally, I can never go back to the phone's physical location and open it. But it sure is fun to call it. Less than thirty days after I did this the phone was replaced. Guess what? The lock mechanisms had the serial numbers stamped on them!

Mr. T.

Suggestions

Dear 2600:

In your last issue you had an article on building a telephone coil which I thought was irrelevant as far as the recording of the red box tones. There is a simpler way of doing this which has worked better. Radio Shack sells something known as a Telephone Pick-up which goes for about $1.99. This plugs in straight to the "mic" of the tape. Obviously, one has to then go to two adjacent phones and do their deed. However, instead of looking for two adjacent pay phones, you can have your mother/father/ brother/ sister/ friend/dog/rat etc. go down to the pay phone and deposit the quarters for you while you stay home and record them on a tape recorder. From experience I suggest using a metal tape for longer duration. Secondly, don't leave this tape in the car or the sun since it may change the pitch of the tones and ACTS will have a hard time picking it up and thus you will be considered a failure.

I enjoyed the tone dialer conversion article tremendously and thought it was a great idea. Keep up the good work.

What I think *2600* should do now is introduce new BBS's. When Central Office and Toll Center were running it was great! The communication between hackers is very important. The next generation of hackers will soon be there to take over and all they will be interested in is "codez". These days the BBS's in the hacker community are generally filled with "codez-asking" kids. No real knowledge is passed on. The Toll Center had rooms to introduce new ones to hacking which was fantastic. Both your bulletin boards networked, which was wonderful. Now the BBS world lacks such boards to call. Think about it.

The Concerned!

We are.

Technical Suggestions

Dear 2600:

Just picked up a copy of your zine at Dark Carnival in Berkeley. Keep up the good work. Some comments on "Hunting for Wiretaps" (Summer 1990, page 24):

Telco does not use series wiretaps, nor does Sprint. The analog hybrid line going into your telephone goes into a SLIC (Subscriber Line Interface Circuit) in the exchange, where a chip called a CODEC (coder/decoder) converts it into a digital PCM (pulse code modulated) stream. This is what actually gets switched in those 5ESS switches Bell likes to talk about. If you are Bell or the NSA, it is a simple matter to order the switch to send you a copy of someone else's bitstream. This is a wiretap in software, for all practical purposes impossible to detect.

Fortunately, most FBI agents know less about the phone system than a dead mule and are equally immune to advice. Twelve volts sounds about right for the analog line while conducting a conversation, but it's more like 100-150V to operate the bell. The lines have a high voltage rating, about 300-500V before the telco surge suppressors cut in and twice that before the SLIC starts to burn. Op amps, on the other hand, have a maximum rating of a hundred volts or so, which is why some lines behave funny when they are tapped (fails to ring or fails to answer when picked up, or very poor audio quality).

The best way to test for an op-amp would be to discharge a photoflash capacitor (330 UFD at 300 volts) into the line and look for the bright flash of light as the op amp went to that great transistor in the sky. But use some caution, as the capacitor is *not* a toy. Get a friendly telco person to unplug the SLIC and tape down the ends of the line with dielectric tape and do the same with your end. Confirm that there is no lineman working on the line or on a nearby one. Then double check. The capacitor is easily capable of killing a human being as well as a fifty cent IC. Don't connect a 300V power supply directly to the phone lines or you are likely to hurt someone - probably yourself. Bleed the voltage off both the capacitor and the line before untaping anything. If you can't

get a telco person to help you out, drop the project. This method is safer than dangling from telephone poles poking at high voltage lines with a multitester, but it is still very easy to fry someone.

As for downing a 747 with a phone call ("Plane Crash", page 31), a lot of the early portable computers were very lax about FCC guidelines for emitted RFI. Think about putting a mobile phone inside an early Compaq or Kaypro and handing it to a passenger as carry-on luggage. Then dial up the box while it's in the air and download a few files. The electromagnetic garbage emitted by the PC could jam the 747 "fly by wire" avionics, leaving the pilots with no control over the plane. If you want a collision, do the deed during takeoff or landing - the 747 will be more likely to hit something. It should be fairly easy for a hacker with a scanner to intercept the fatal call, although identifying the guilty party might be more difficult. Perhaps your hacker can read the packet headers and trace the call? Or his girlfriend is a cop and she traces it for him?

AP
Oakland, CA

Caller ID Override

Dear 2600:

From what you know about the caller ID systems that are gradually being introduced, do you think it would be possible to build a circuit or add-on box to your own home phone to send a false number to the party you are calling? It would seem to be the ultimate defense against the invasion of privacy while at the same time giving the appearance of cooperation without a "P" for privacy showing up on everyone's caller ID screen.

Pete
Akron, OH

Absolutely. We hope to see someone do this soon.

A Phone Company Tour

Dear 2600:

I had the opportunity recently to tour the 4ESS owned by AT&T here in Cincinnati. I went along with a tour offered by the local chapter of the American Society of Mechanical Engineers. It was an interesting office, because four or five different levels of technology were present in the same building. These ranged from hardwired, dedicated lines leased by companies and corporations for direct data or voice communication between distant locations (Saks Fifth Avenue can pick up a phone here in Cincinnati and immediately ring a phone in the New York office without actually making a long distance call). I gathered that this was a pretty expensive option and would only pay off if you made a hell of a lot of calls to the same long distance point. This system was still using the old style plug-and-socket boards that were the rage earlier this century.

There were no mechanical switches in use, but there were several levels of electronic switching ranging from large, outdated analog circuit boards to the new fiber optic system that they were still in the process of installing. The whole system was backed up by a roomful of massive wet cell batteries that would supposedly keep everything humming smoothly for about eight hours after a power failure.

I was surprised to find that there are only 15,000 outgoing long distance lines emanating from the Cincinnati 4ESS. I had suspected that there were many times that number since this is such a big area with so many customers. I was also amazed at how small the cable cluster coming into the 4ESS from the Cincinnati area central offices was. I would estimate it to be only a couple of feet in diameter and it was entirely unprotected once it entered the building. (I hope no terrorists are reading this.)

The AT&T fellows were quite knowledgeable and informative. They even attempted to go into a little switching theory; obviously thinking that a group of mechanical engineers would be appreciative of such information. I was, but my fellow engineers were busy asking questions like, "Is there really a single wire that runs from here to California that you talk over?" and other questions similarly asinine and inane. I was embarrassed for them and hid my head in shame.

I totally struck out in asking questions about the ANI for this area, and in wondering aloud why the phone company charges for touch tone service when the whole bloody system is based on those magical little tones. I, of course, scanned all visible paper for phun numbers, but everything was well hidden. My mouth

watered when I saw the full set of operational manuals for the 4ESS sitting out in the open.

A major alarm went off in the system while we were listening to switching theory. It seems that someone dug into a large and rather important cable cluster somewhere in eastern Cincinnati, thereby cutting three or four central offices off line for a while. The technicians on duty knew what had happened in about fifteen seconds after the printers started dumping trouble codes. One of the guys even let us peer over his shoulder as he accessed one of the downed connections and did some diagnostic checks. Pretty neat, that.

Well, enough about my little tour. Now to some suggestions for future issues: program listings for an IBM compatible computer for a blue box, a red box, and some dialing programs (modem searches, extender searches, etc.); comprehensive listings of exchanges other than New York area; ANI and CNA (with access numbers) for the 513 area code; more BBS numbers; book reviews; equipment reviews (scanners, pen registers, phones, computers, and other things that can be used for hacking and phreaking); more hands-on information; and information on ATM machines and their ilk.

Mitch
Cincinnati

Assorted Thoughts

Dear 2600:

In my area, Ma Bell finally improved one of their long abused holes: they got rid of the operator for collect calls. One can no longer bill to another number or make a collect call with a human operator. Instead the system will ask for your name and digitize it and play it to the destination to verify the billing. So the person you're billing will probably recognize whether or not the person is actually who s/he claims to be. It sure took them a while to figure that out.

Anyhow, with this procedure one can also make five cent local calls from public pay phones. The good part is that it's completely legal. Just bill the destination and when the system asks for a name, say the phone number of the pay phone. Hopefully the person who picks up on the other end has some common sense and calls you back. So now you don't have to carry around any change and you still save yourself a good twenty cents (it does add up eventually!).

By the way, Sprintnet (also known as Telenet) is doing some sort of deal with transmitting data in printed form to addresses via US mail. Does anyone happen to know how to access it? I'm using it through a net but it's too expensive. I'm pretty sure there's a way to do it directly.

Keyboard Jockey

Call 800-TELENET and ask them about that service. MCI Mail has something similar if not identical. You can always use an operator for collect or third party calls if you don't have a touch tone phone or if you say you don't.

Dear 2600:

I really don't want to write another one of those "Gee, I really really like your magazine...." letters, but unfortunately that is exactly how I feel. I am in my mid twenties and way, way back in the silicon dark ages (put it this way, I can remember when the IBM PC was thought by some to be a flash in the pan that would never oust the Apple II as the market leader) I discovered computers and modems. I had a second-hand Apple II+ (which I still use with pride and some choice hardware enhancements), a Hayes Micromodem II (since upgraded to a Practical Peripherals 2400 external), some "borrowed" software and a lot of naive curiosity. I was never a "hacker" per se, since I have about a third grade computer literacy level and the extent of my hardware knowledge is knowing what card plugs in where, and I did do some things in that dark time right after the breakup of the phone company that some water under the conscience tells me were not too nice, but I really didn't know any better.

With my little toy I discovered a whole new method of communications, with the immediacy of a telephone call and the depth of a letter to the editor. It also opened up the world of everyday technology: I heard about the rainbow of boxes that certain people use to test the limits of the phone system that 99.9 percent of people (myself sometimes included) take for granted. I heard about different computer systems and how to get into them. Frankly, I've never really wanted to hack myself, but it's always been fun to find out how I could do it, and stories from those who did such things were always fun to read.

In short, I experienced what the framers

LAST OF THE LETTERS

of the U.S. Constitution had hoped for when they sat down in Philadelphia in 1787: the free and open exchange of ideas (to borrow from WABC's Bob Grant). Even if the information shaded a little to the gray, it was still useful. But, freedom and paranoia go hand in hand: if you are free to do what you wish, eventually the exercise of that freedom may impinge upon the freedom of someone else. That is why we have laws, some fair, some not. Now, I'm not saying that laws cause criminals because there is a certain percentage of humans who will always do things at the expense of other humans, but I do believe that unfair laws will awaken otherwise latent tendencies in people. Since people will increase their "law-breaking" in the face of unfairness, those in power will retaliate with tougher laws, and so it spirals up until it can go no higher and suffocates in the stratosphere of social collapse.

What does this have to do with *2600*? Your publication is one way responsible citizens have of combating the unfairness in our post-industrial society. Since information has become power in our society (witness the inordinate influence that CNN has over government policy), those in power, whether they are government or business, find it incumbent upon themselves to control what people know. Fortunately, we live in a more-or-less free society and we can get access to information *if we dig for it*. There is enough self-incriminating information spread across all of the U.S. government's own pamphlets and press releases to keep self-appointed "government watchdog groups" in Brooks Brothers suits, but that information is not publicized. So maybe the key to our so-called "Information Economy" is publicity. Sure, IBM gets all the publicity for marketing a bug-ridden, hard-to-use computer, and Apple Computer can "Win the Hearts and Minds" of computer users, but who outside of semi-hardcore computer buffs know about the Amiga, or even Steve Jobs' neXT? They can blow the disk drive doors off even a fully-loaded IBM power user's dream machine, but who's really heard of them?

So this isn't the "Information Age", it's the "Publicity Age". As Adolf Hitler said, if you must lie, tell the most outrageous lie you can. It's easier to believe that way.

The Disco Strangler
South River, NJ

COCOT Info

Dear 2600:

Thought you'd be interested in the following. I called the COCOT you listed (212-268-7538) and noted it answered with a computer tone and an ASCII blip. Upon recording this blip and playing it through a computer modem, the following was generated:

T:@*2122687538*33725*CA2107*8934*087*9012216073424*00000-

Attempts to hack into the COCOT resulted in being disconnected. I could not get any kind of response other than the above at initial connect. This was done at 300 baud.

Waterbury, CT

Dear 2600:

This is just a little something interesting we've discovered. The phone numbers (both in the 212 area code) are the ones which appeared as a response to a letter about the article on COCOT's which appeared on page 31, Autumn '90. The two numbers connect at 300 baud and send the following alpha-numeric strings.

212-268-6129:
T:@*2122686129*41465*CA2202*6837*142*9101116171141*00000E

212-268-6129:
T:@*2122686129*41465*CA2202*6837*142*9101116171205*00000D

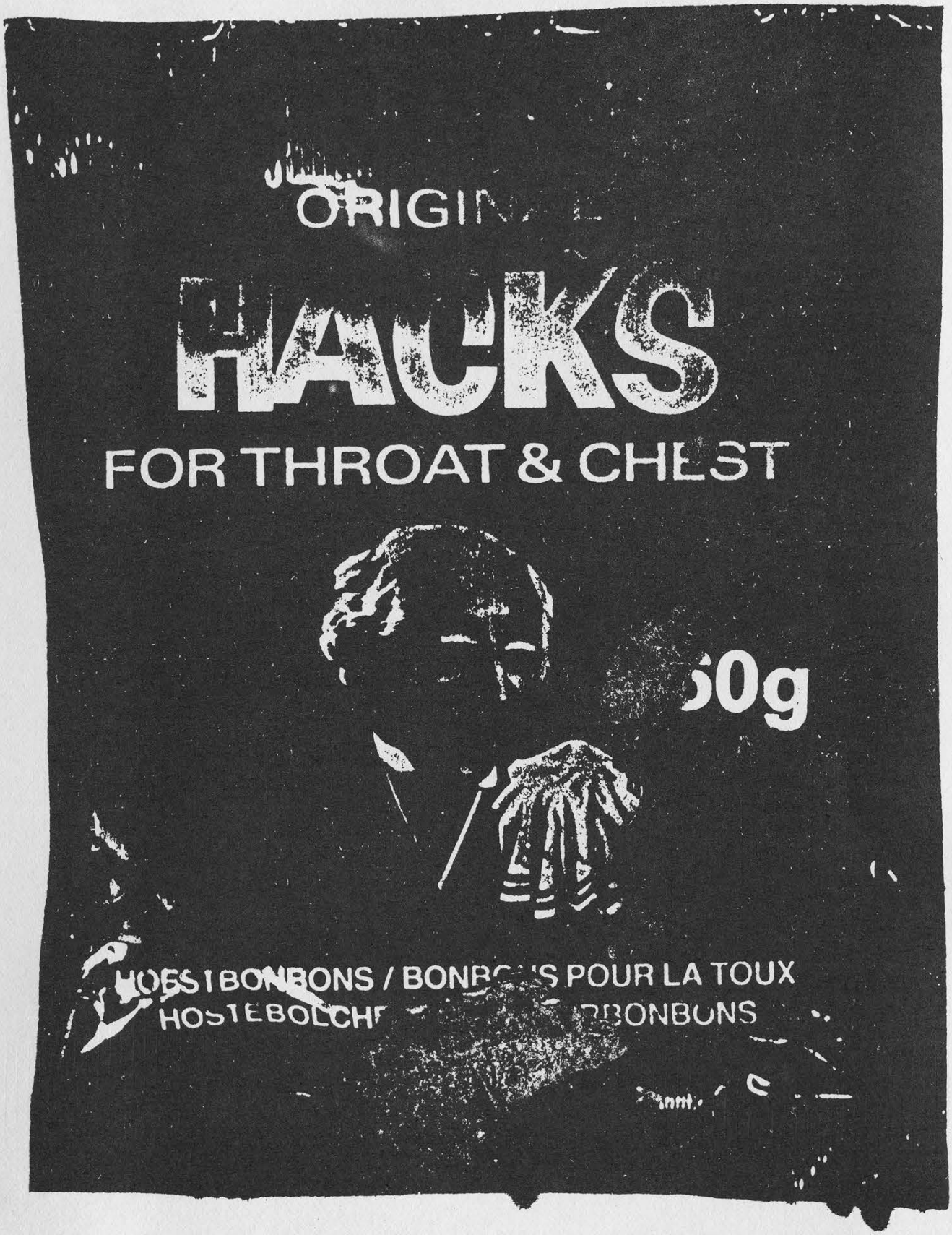
212-268-6129:
T:@*2122686129*41465*CA2202*6837*142*9101116171228*00000?

212-268-7538:
T:@*2122687538*51880*CA2202*7637*222*9101116171435*00000

The Martyr and
The Mute & Bach Wai

Now this is what we like to see. Readers taking it upon themselves to go further with the information we print. Is there someone who can explain what these numbers mean?

2600 is always in need of writers!
If you've got a field of expertise or a story to tell, send it in to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953
Questions?
Call (516) 751-2600



CAN YOU BELIEVE THE THINGS PEOPLE SEND US?

OUR CONTEST

In our Summer 1990 issue we published a bunch of negative letters that were written about hackers. We invited our readers to come up with replies. The winner would get a free lifetime subscription. We got a pile of really good entries. And when the dust cleared, we realized that we had two winners. Unfortunately, neither of our winners did a very good job of identifying themselves. So we have absolutely no idea where to send the subscriptions. If you recognize your piece below, contact us and think of some way to validate your identity.

Entry Number One
by TELEgodzilla

I found the Summer 1990 issue very intriguing - particularly the section dealing with the other point of view against those who attempt to learn more about systems. As I was reading these letters of anger, shame, and disgust, I was struck by how similar this situation is to what Dr. Richard Feynmann experienced during the development of the first atomic bomb.

In the book, Surely You're Joking Mr. Feynmann, there is a chapter relating how Dr. Feynmann was able to crack open U.S. Army safes which held the plans and makings of the then being developed atomic bomb in Los Alamos (chapter entitled "Safecracker Meets Safecracker", pages 119 to 137, Bantam Books). Feynmann had discovered, after speaking with a safecracker, how most safe factories give a standard assigned combination number to safes, instructing the buyer to reset the locks. Most buyers, however, didn't bother reassigning their safes with new combinations, failing to realize that the standard assigned number was just that - a standard assigned number for *all* safes then being made. What Feynmann did was go around and open the Army's safes within the Los Alamos compound (he was able to open one out of every five) with little trouble for nobody had thought of bothering to change the combinations after the safes arrived from the factory!

How was Feynmann treated? With respect and understanding? On the contrary - he was nearly thrown out! Did the Army change the safe combinations? Sure - eventually, but not until after several months into the project.

So you ask yourself - what the hell was Feynmann doing? Couldn't he just leave well enough alone?

No; Feynmann had a curiosity - the very same curiosity which led him to develop new and better understandings of the atomic sub-structure led him also to find ways in which to open up Army safes.

This is the crux of the argument and controversy surrounding hackers: people are naturally curious. Trying to stop this curiosity from enveloping the world around us is akin to trying to stop a mountain of water. Even if we did, it'd only bring about more trouble (besides developing new and wild forms of nervous neurosis), for man is differentiated from animals on many points - and chief among these points, curiosity rules the pack.

It's fascinating, but none of these letters spoke of harnessing the very same curiosity and drive toward protecting their systems. Instead, we all merrily throw things about, rant and rave about how terrible it is for people to go "walking through their house" without stopping and considering how to find out ways of positively utilizing the skills and powers of those capable of doing so.

But an even more important point not being raised throughout any of these discussions is the fact that perhaps privacy is nearly dead - and it ain't by those "kids".

When you stop and consider how many files the U.S. government has on each person - whether you're in the armed forces, receiving or have received a college loan, possess a driver's license, hold a social security card, maintain a farm or a grocery store, pay taxes on a regular basis, etc. - the fact of the matter is that there are bigger and more nasty people who rummage through your house on a regular

WINNERS

basis - and *you don't even realize it!*

Protection of our credit records is probably one of the greatest non-issues today. TRW or Dunn and Bradstreet regularly sell information on your credit status and income standing to corporations which seek only to find new markets to sell their products. *It's a point of rule that every time you receive junk mail, somebody accessed your credit records.*

And we're worried about punk kids taking a walk through telephone companies to get information that they could receive by the mail for $13 - as the Neidorf case proved?

Somehow the real criminals are getting away scot-free.

I respect people who take the time and effort to find ways into computer systems, for we all learn much from it; it keeps us on our toes. And in this apathetic society I also feel better when I know that there are people who *do* care about the world around themselves and take the time and risks upon themselves to learn more.

That's not only curiosity, that's entrepreneurship. Equality is never something given; it is only achieved and maintained through diligence and persistence. Having information hidden away is anathema to democratic freedoms. Seeking out information makes us grow and become more competitive on the world market; this is what makes our country great.

As a professional operative, I think many of these people would be mildly shocked if they found out to what extent and degree private and public institutions employ people such as myself, and how much information is constantly available on the average citizen.

I have little regard for those who brand "hackers" as threats for no other reason than for their impassioned curiosity. Grow up yourself! This is a bigger world than you realize and, as a professional, I frankly find this talk of anger to be utterly misdirected and somewhat naive. Attack TRW, Exxon, the Republican Party.... Any corporation - public or private - possessing of multi-faceted interests is inevitably going to have some sort of computer system and with that system are those who are going to make sure that it works - even if that system is meant to take information about your checking account, car insurance payments, psychiatric care, or even if you had recently purchased any Elvis records!

It is not surprising that the majority of these hackers are young. We should come (and pray) to expect more of these individuals to arrive into prominence, for we are a country that is losing touch with its people, most particularly its youth. Here we stand, bitterly complaining how many youths cannot read a map (much less actually read) and yet we have those able to discover new means of accessing information which even the so-called "experts" never realized existed!

We are punishing talent that this country desperately needs, rather than reaching out to exhort this raw and excellent energy into new and vital means beneficial to all - particularly those who possess this great inner strength.

No, don't go for the kids who rummage through your garbage; go for the faceless professional bastards who keep and maintain a detailed profile on you so that they can sell you watches, cars, beer, and, yes, political issues. For it is they - those who maintain those giant mainframes without even *bothering* to think about the consequences (as well as those who rule) that we should be watching.

The child who discovers that the emperor is nude should never be punished. It's time that we start noticing these little details.

Entry Number Two

I'm a hacker. I worship the computer and the endless possibilities it poses. I see programming as an art, and I was born to explore. When I sit down at my computer to do something, I don't debate in my mind whether or not what I'm doing is illegal or

unethical. I just do it. The computer is a medium which is so immediately explorable, with a scope so infinite and a depth so limitless that it makes "just doing it" extremely feasible. That being the case, there is more to a computer than programming, and those with an insatiable instinct to learn and know easily assimilate themselves into the abundantly different aspects of the computer world and, inevitably, into aspects associated with underground activity. This type of person, the hacker, does not think in terms of right or wrong, as the definition of these terms depends on how you look at life in general. The means is the ends, and the ends justify the means. Columbus was a hacker. He explored new worlds because they were there. He didn't stop to wonder what effect his discovering the New World would have on the Native Americans. He just did it. Leonardo daVincci was a hacker. He explored the human body, among other things. In his time, it was forbidden by the church to dissect dead bodies to find out what made a human tick, but he couldn't care less what the church had to say about it. He had a desire to know, so he just did it. Humanity has a history of wanting to know and this desire to know sometimes leads to questionable means. Questionable, depending on how you look at it. If it wasn't for the hackers of different sorts throughout history, where would humanity be now? Although we probably wouldn't still be dressed in animal skins if people had always remained complacent to those in authority and shied away from those things that we "weren't supposed to do", we wouldn't be as nearly advanced a civilization as we are today. It's because of those people who dared to know and had the desire to understand the world around them that we are at the point in history we are today. We owe a lot to hackers.

Although I'm not a gung-ho systems hacker, I've done enough to understand the thrill and relish the challenge. I was once under surveillance by the phone company for "being where I shouldn't have been," so I feel I'm at least that much more qualified to comment on this subject than your average Joe computer user. It's called experience, and that's something I have a fair amount of due to that peculiar instinct we all have inside of us called "hacking".

Some people believe that when you hack you are going somewhere you do not belong and equate this to breaking into someone's home. This is a stupid analogy that is much overused. Hacking is a game as much as life is a game. If you choose to play, you accept the risks associated with it. If you win, you win, and if you lose, you lose. What are the rules? What are YOUR rules? You play the game as you wish and you deal with the consequences as they come, and only your conscience and personal integrity dictate where the game leads.

Scenario: You break into a house and you start looking around for something interesting that will tell you about the owner. Many things can happen at this point, one thing being the owner of the house wakes up and finds you rummaging through his file cabinet, whereupon he pulls out a .357 magnum and blows a two-inch hole through your chest and you die.

You can see how the analogy between hacking into a system and breaking into someone's house doesn't hold up too well when you really put any thought into it. When someone goes through the trouble of breaking into a home it is usually for malicious intent (i.e., to burglarize, rape, etc.) and rarely just to dig through personal files (which is not the definition of hacking anyhow). Hacking is something you do casually in the comfort of your own home. With the majority of hackers, there is little likelihood of any intent to do harm, but rather an innate curiosity. Can the same be said of a burglar or a rapist walking into an unlocked home? Someone breaking into a residence usually has premeditated a crime. A hacker is merely exploring. If, in the process of exploring, a very tempting bit

OF THE HACKERS

of information is found, the hacker must make a decision: does he download the file or leave it be? If you go to buy a newspaper from a machine and find that the last person to purchase a copy left the door open, do you take a copy without paying for it? Nobody would probably ever know if you did or not, so the question comes down to your personal ethics. Do you take it or leave it? What are your rules?

Scenario: This strange system you've just hacked into turns out to belong to one of those mailing list companies that sells your personal information to those annoying sweepstakes and mail order firms. Is it alright for them to sell your personal information and for you to be looking around in their files? Is it wrong for them to be selling your personal information as well as for you to be looking around in their files? Neither? Either? Both? What are your rules? They're making money, which they enjoy, and you're learning the system, which you enjoy. Are they wrong for wanting to make money? Are you wrong for wanting to learn? What are your rules?

Now let's say you've done something particularly heinous, such as broken into a Bell South computer system and heisted some file called something like "E911 Overview" which is purported to be worth around $79,449 (actually, $13 with a $79,436 legal fee). Eventually the all-powerful and all-knowing Secret Service, that institution of unfathomable intelligence, tracks you down and decides to smite thee and all in your path with its mighty wrath. Well, now you've been caught. You played the game and landed on "Go To Jail", and you ain't passing go, baby. You took the risks and lost...but the game is more complicated than that.

Since we all have to participate in this game whether we like it or not, it is necessary to explore the effects of this broad-scoped action taken by the very government institution which we entrust to protect our God-given rights. The minute details cannot be ignored, as they are the scariest and speak the loudest in terms of criminality and injustice. Yes, even more so than that evil 19-year-old punk with the ego.

This treasure dubbed the "E911 document" makes its way through numerous systems via a network, unbeknownst to the owner of each particular system. The SS (Storm Troopers), while tracing this document's trail, come across one system that the document made its way through. To them, it's obvious that this system was involved in this plot to disable the emergency phone system and lead to the downfall of the government, the country, the world, and then eventually life itself. So they see no problem with confiscating this system and everything else that looks suspicious inside the abode where it dwells: the disks, notes, books, magazines, music tapes, stereo, TV, lamp. No, not even the toaster is immune from this rampage. Hey, it's got a cord on it; it *must* be involved in this devious scheme somehow! Maybe the person being stripped of all his possessions and dignity at this moment, who in all likelihood is being physically restrained by four men in dark sunglasses, his poor mother in handcuffs with a double-barrelled shotgun pointed at her head (she just *might* try something, you know) is some undiscovered super-genius who has developed a method of encoding data on toast. They want to check those bread crumbs at the bottom just in case.

Scenario: Someone who has just burglarized a home runs through your yard as he attempts his getaway. The cops trace his trail through your yard. Are you now guilty by association? Do the cops rampage into your house with destructive force, confiscate all your possessions and terrorize you and your family members to gather evidence that proves that your neighbor's house had been burglarized? No. Is this analogy more suitable than the one so commonly overused by those who

(continued on page 46)

We've published information in the past on AT&T's USA Direct. Out of fairness, we should tell you that there are other similar services that allow you to call back to the United States from other countries without having to deal with local operators who often don't have the common decency to speak our language. You can now avoid foreigners on the phone by using Sprint Express. You'll be connected with a Sprint operator in the United States who won't disrespect you. Some countries and the numbers to call from them: Argentina: 001-800-777-1111; Australia: 0014-881-877; Chile: 00, wait for tone, 0317; Colombia: 980-13-0010; Denmark: 8001-0877; France: 19, wait for tone, 0087; Hong Kong: 008-1877; The Netherlands: 06, wait for tone, 0229119; Japan: 0039-131; Singapore: 800-0877; United Kingdom: 0800-89-0877. All of these connections are toll-free. You can bill calls to a FON card, call collect, or use your local calling card.

***

There's also a new Sprint service that allows you to conference calls. It only works on FON card calls and not on 10333+ or 950-1033 calls. When connected to a call, hitting a star for a full second will put you in conference mode. You can then dial 12 which puts the first call on hold. Then you dial the area code and number of the second call. After the second call answers, you hit another star for a full second, then dial 13. The second call is now linked to the first. If you want to disconnect the second call without linking it, dial 14 instead of 13. There's a 75 cent surcharge on top of the regular FON card surcharge (times two) on top of the charge for the two phone calls. Maybe someday they'll finally get it right.

***

Allnet has a whole host of services they've been introducing. By calling 800-783-1444, you can place calls by dialing 0 plus the number followed by your Allnet calling card number. Or you can dial a two-digit "Speedlink" code followed by a star and then your calling card number. This will connect you to a variety of airlines, hotels, and car rental establishments, all of which have toll-free numbers already, so you'd have to be kind of crazy to spend 20 cents a minute using *this* service. If you hit a star after connecting to Allnet's 800 number, then enter your calling card number, you'll be able to access InfoReach (recorded announcements on the stock market, horoscopes, sports, entertainment, and international time and weather costing between 30 cents and 70 cents a minute), Call Delivery (for $1.60 you can record a brief message for immediate or future delivery to any phone number in the U.S.), Voice Mail (with a 7-digit ID number and a rate of 38 cents a minute), and Teleconferencing ($2.00 for the first minute, 49 cents a minute for each caller). In its little brochure, Allnet urges its customers to "power dial" and save. What does this mean? It's rather frightening, actually. It seems that Allnet now charges calls from the moment you access the Allnet dial tone. (They swear they won't charge you for uncompleted calls.) Allnet says, "Don't wait to hear every word of a prompt or the end of a tone before you continue dialing. If you know the next step, start dialing as soon as you hear the beginning of a prompt or tone. It saves time, plus you won't be charged for time spent listening to instructions you don't need." This is the first case we're aware of where a long distance company blatantly admits charging its customers for the time they spend *dialing* the call.

***

Allnet also has an international call-back service like USA Direct and Sprint Express. They call theirs Option USA. The countries and numbers are: Australia: 0014-800-125-197; Belgium: 118671; Denmark: 8001-0658; France: 05-90-2919; Greece: 00800-12-2100; Hong Kong: 800-6159; Israel: 00177-150-1067; Italy: 1678-97038; Japan: 0031-12-2453; The Netherlands: 06-0228491; Spain: 900-99-1450; Sweden: 020-79-3934;

Switzerland: 046-05-8812; and United Kingdom: 0800-89-2695. Canadians can access Allnet by dialing 800-955-1444.

***

With all the fussing and fighting in this country over Caller ID, it's interesting to note that British Telecom *refuses* to provide the service. While privacy may still hold some appeal over there, so do rip-offs. Several companies have sprung up offering CLI (Caller Line Identification) devices even though it's technically impossible since British Telecom doesn't pass along the number of the calling party. So how do these companies manage to make these offers? Their devices simply ask the caller to enter his/her phone number before the call is completed. Lo and behold, the number that the person entered is displayed on the called party's magical device as soon as the phone rings. And the person can enter any number their heart desires. In other words, this is about as far from Caller ID as one can get.

***

According to an internal NYNEX memo, the systems known as COSMOS (provisioning) and TIRKS (trunk assignment) will be replaced by the new Bellcore-designed system known as SWITCH. "It's time to take advantage of the advances made in computing technology" over the past 20 years, say the people in charge. SWITCH, which stands for absolutely nothing, is scheduled to be installed in late 1991, with implementation to follow a year later. The new system is actually divided into two parts: SWITCH is the "provisioning" part of COSMOS and will require synchronous terminal access, whereas FOMS, the frame work management part of COSMOS will require asynchronous terminal access. All current COSMOS users in NYNEX and its children (New England Telephone and New York Telephone) will be getting a "network terminal survey" to evaluate the needs of the future. SWITCH was first mentioned in *2600* a while back but it now seems close to reality. We imagine similar plans are being made all around the country.

***

According to the Amsterdam (NY) police department, a former resident "known for causing mayhem with telephone and computer lines" has been connecting their phone lines to people all over the world and billing it back to the police. "We pick up the phone and we've got the Los Angeles sheriff's department on the other end," they say. Newspaper reports claim the villain is able to gain access to the "telephone computer system and use the police department's access code". The translation of this is that he/she is able to get and use a calling card number. According to a friend of this nasty person who contacted *2600*, the police have "harassed my buddy for years. Now there's a war between [this person] and the police...for over two years. My friend is a notorious hacker."

***

If you're a gang member in Los Angeles, you may get to take part in an exciting new technology experiment. Whenever there's a hint of trouble in the area (gang wars, retaliatory strikes, etc.), known gang members who are also on probation will be placed under electronic house arrest. These subjects will have created a "personalized template" by repeating the names of 22 states three times in succession to a computer. The computer will then call the gang member at a random time and ask him to repeat eight states. If he doesn't pass, it will call back to give him a second chance. If he fails again, the computer calls the probation officer's beeper. And a recording is made of the failed response. Our question is this: don't most gang fights take place late at night? If a gang member has to stay home instead, maybe he'll want to go to sleep at a normal hour. But how can he when he's going to get a phone call from a computer? Also, what happens if the phone is busy? Is using the phone going to be illegal during house arrest? Will call-waiting become mandatory? And what if the gang member is using a modem? Will call-forwarding be

illegal? And what happens when a clever gang member invents a voice recognition system that is able to generate a response in his voice when it hears the name of a state?

***

Hi tech is also coming to the rescue of police/informant relations. By dialing into a computer system called CASSIE SX-4, informants can leave messages for their police contacts. CASSIE will then page the police officer. Ross Distributing of Upland, CA claims the system will provide more security because "only the officer knows his password". For $4000 you can get software that can handle up to 75 mailboxes. You'll still need an AT compatible computer. For around $15 a month you can get a single line voice mailbox through the Yellow Pages that does basically the same thing.

***

The next time you get all frustrated at a payphone, think of this: the cost of a local call at a payphone in Poland was recently raised to 20 zlotys (still less than one American cent). But 20 zloty coins have become a scarce commodity since they're in such demand. There are two other sizes of 20 zloty coins that can be found quite easily. But they don't fit into the phones. There's also a 20 zloty bill but that doesn't fit into the phone either. So what do people do? What else is there to do in Eastern Europe but make use of the black market! There you'll find all the 20 zloty coins you need — at a cost of between 200 and 1000 zlotys apiece.

***

Illinois Bell is applying for Caller ID. The following excerpts come from the December 1990 issue of Illinois Bell's Telebriefs newsletter: "Illinois Bell believes that a person who receives a phone call is entitled to the same information as the person who makes the call, namely the phone number of the person at the other end of the line....Illinois Bell is proposing to offer Caller ID without the blocking feature that some groups have proposed. With the blocking capability, abusive callers would be able to prevent their numbers from being displayed, thus diluting the benefits of Caller ID.... When it is necessary for individuals to maintain their anonymity, operator assistance, calling cards, public phones, and cellular phones can be used." What they don't seem to be taking into account is the fact that abusive callers can take those very same steps to maintain their anonymity. Since it's technically impossible to identify someone who uses the above methods, very few abusive callers will continue to dial direct. Which leads us to believe that, despite their sales pitch, Illinois Bell is really interested in Caller ID'ing all of the non-abusive calls. Of course, if they phrased it that way, people might just think twice.

***

New Jersey Bell has really pulled one over on the public. Remember when 900 numbers first started being dialed en masse? New Jersey Bell, and most other local phone companies, told us not to worry; it was easy to block such calls and it didn't cost anything. Now if you want the privilege of not being ripped off by 900 and/or 700 numbers you have to pay a one-time fee of $5. Then there's another one-time fee of $16 to process the order! Businesses have to pay even more. In all likelihood, less than ten keystrokes are required for the whole order. It's bad enough to see so much cheating going on in the phone business, but ripping you off to protect you from being ripped off is more than most people deserve.

***

Some British statistics: More than 99 percent of the 80 million calls made every day get through on the first try; about 90 percent of calls to "directory enquiries" get through on the first try and seven out of eight of those are answered within 15 seconds; ninety-six percent of British Telecom's 95,000 public telephones are in full working order at any one time; and, on the average, a "fault on a line" will occur only once every six years.

our exciting world

According to British Telecom, "Nearly 11 million customers are now connected to local digital exchanges. And more than 70 percent of customers are served by modern digital or electronic exchanges offering faster connections, clearer lines, and fewer call failures.... Unfortunately there are cases where we fall short of the high standards we set ourselves. To put things in perspective, even if we fully satisfy 99.9 percent of our 25 million customers, we will still have 25,000 who are disappointed."

***

The British have also done away with an unfair charge that we in the States still contend with. There are no longer connection charges for customers who take over an existing telephone line without a break in service. In other words, if you move into a house with a phone line already installed, you won't have to pay for the phone company to switch the account to your name.

***

A couple of other British tidbits from phone company publications: "Push-button phobia is stopping millions of people getting the most from their telephones. Almost half of British Telecom customers have digitally-connected homes, but few know, or try to find out, how to take advantage of all the phone's functions. For example, the cost of BT's operator-alarm service has doubled from 1.20 pounds to 2.47 pounds but for just 13p a call you can programme your phone to wake you up. Simply pick up the receiver and dial 'star 55 star' followed by the time you want, using the buttons on the phone's tone pad for hours and minutes. To check you've got it right press 'star gate 55 gate' and the exchange's synthesised voice gives the alarm time. To cancel the alarm call simply press 'gate 55 gate'." But all is not well in the U.K. This letter recently appeared in The Sun: "British Telecom services have improved immeasurably since it cast off the shackles of State ownership. We may not like the new telephone boxes, but at least they work. The company still gets complaints, but at least it responds to them. So we hope it will reconsider plans to charge 35p for Directory Enquiries. BT is now ringing up profits at the rate of 8 million pounds *a day*. It has a duty to shareholders, but must not forget that although it is a private company it is still supposed to be a private service."

***

About the most useless thing we've seen in a very long time is the AT&T Callers' Club. It came in the mail a couple of months ago demanding attention. "You've already earned your membership just by being a great customer. There's nothing more you need to do, and no strings attached." There also seems to be virtually nothing this "club" has to offer. There are promises of "previews and discounts for new AT&T products" like Voicemark, AT&T's messaging service that we wrote about last issue. We doubt AT&T won't tell "non-members" about their new services and so far we have yet to see any discounts that couldn't be obtained in the real world. We're also privy to announcements of "AT&T sponsored events" in our area. Wow. Unless that includes hacker raids, we're not impressed. A chance to win "fabulous prizes" and "valuable savings". Again, nothing we haven't heard before numerous times. Finally, a toll-free number reserved for "members only" (800-223-2000). We can use this exclusive number to "find out about discount periods and calling plans, receive immediate credit for misdialed calls, ask about your bill, get prices for the cost of a call between specific locations, order your AT&T card, learn how to access AT&T when you're away from home, and notify AT&T when you move, so that you can continue to receive your Callers' Club benefits without interruption." We are flabbergasted. There is *nothing* here that you can't already get by dialing customer service (800-222-0300) or your AT&T operator. We don't know what AT&T is up to with this gimmick but we'll keep everyone informed. By the way, they sent everyone a

(continued on page 44)

To Our New York Telephone Customers

Beware of Telephone Fraud!

Recently some unscrupulous people—posing as security officers from New York Telephone or other telephone companies, or identifying themselves as federal or police investigators—have tried to deceive and cheat New York Telephone customers. With the excuse of helping them in their "investigations," these "agents" ask you to accept the charges for phone calls from people that you don't know and in some instances they even threaten law suits or suspension of your phone service if you "don't cooperate."

Please, DON'T FALL INTO THIS TRAP. Don't let strangers charge calls to your phone number. New York Telephone is **not** asking for its customers' help in catching crooks.

DON'T BE FOOLED by these impostors that have nothing to do with New York Telephone. If you have questions or doubts, call your New York Telephone Business Office at the number that appears on the first page of your telephone bill. We're here to help.

We're all connected.

New York Telephone

A NYNEX Company

WE DON'T KNOW WHAT'S GOING ON, BUT RECENTLY EVERY CUSTOMER OF NEW YORK TELEPHONE GOT THIS NOTICE.

2600 Marketplace

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

RESEARCHER/WRITER seeking inside information on credit bureaus for story on privacy issues. Please call 301-702-1009 after 6 pm, ask for Edward or write: 3311 Dallas Drive, Temple Hills, MD 20748.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

FALCON would like to trade knowledge and codes with other hackers. Also interested in trading the latest videos, music, etc. Falcon, PO Box 1038, 7550 BA, Hengelo, The Netherlands.

CONTROVERSIAL DTMF DECODER as shown in the Spring 1990 issue. Exclusive offer to 2600 readers: complete revised plans with layout and explicit instructions for construction. Information and hardware commercially sold for $$$. Sending a SASE (with .75 postage) nets you 9 pages of data for the stamp!!! Decoder chip and PC board available. W.E.B., PO Box 2771-H, Spring Valley, CA 91979.

ANTI-WIRETAPPING bug detection, privacy protection, information services, new and used equipment. State of the art equipment beyond today's technology! National computer search system, information research service. Retail/wholesale, surveillance and countermeasures equipment. Call E.C.I. Free consultation hotline: (516) 929-3261.

LOOKING FOR SOMEONE to correspond with to get a basic understanding of hacking and phreaking. (I am in prison.) As I would like to ask questions, please write me directly. If you wish to use a nickname that's fine. Just make sure you write it as your return address or it won't get to me. Victor Mendoza, 9601 NE 24th St. 410216, Amarillo, TX 79107-9601.

OLD TAPES of telephone recordings, rings, busys, etc. wanted for radio programs. Also, current recordings and funny phone calls welcome. Send to Emmanuel, PO Box 99, Middle Island, NY 11953.

WANTED: Red and blue box plans/kits and assembled kits. Also, expansion cards for a 256K Compaq. Please contact Charles Silliman, 11819 Fawnview, Houston, TX 77070.

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

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

WANTED: Atari ST hacking/telecom programs to trade. I have Mickey Dialer and 2 tone generation programs. Nil, PO Box 7516, Berkeley, CA 94707.

Deadline for Spring Marketplace: 4/1/91.

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.

PUBLICATION DENIAL NOTIFICATION

TITLE OF PUBLICATION 2600 Magazine Fall 1990 V7 N3

The above publication has been reviewed and denied in accordance with Section 3.9 of the TDCJ Rules and Regulations for the reason(s) checked below:

- ☐ (a) Publication contains contraband.
- ☐ (b) Publication contains information regarding the manfacture of explosives, weapons or drugs.
- ☐ (c) Publication contains material that a reasonable person would construe as written solely for the purpose of communicating information designed to achieve a breakdown of prisons through inmate disruption such as strikes or riots.
- ☐ (d) A specific factual determination has been made that the publication is detrimental to prisoner's rehabilitation because it would encourage deviate criminal sexual behavior.
- ☒ (e) Publication contains material on the setting up and operation of criminal schemes or how ro avoid detection of criminal schemes by lawful authorities charged with the responsibility for detecting such illegal activity.

REMARKS Pages 18, 19, 20, 21, 29, 42 and 43 contain information on misusing telephone equipment to make telephone calls illegally and to obtain cash and credit cards illegally.
(Does not qualify for clipping.)

If there is a desire to appeal the rejection of the aforementioned publication, this may be accomplished by writing to the Director's Review Committee, P.O. Box 99, Huntsville, Texas 77340. The appeal must be mailed so as to arrive at the Texas Department of Criminal Justice, Institutional Division, within two (2) weeks of the date shown below

MAIL SYSTEM COORDINATORS PANEL

January 9, 1991
Date

2600 Magazine
Publisher / Sender

P.O. Box 752
Address

Middle Island, NY 11953
City, State, Zip Code

White
Canary
Pink

1193 Rev. 1/90

YOU CAN BET THIS WENT RIGHT UP ON THE WALL THE MOMENT WE GOT IT. WE'D LIKE TO KNOW WHAT OTHER MAGAZINES HAVE RECEIVED THIS HONOR. AND HOW MANY MAGAZINES CONTAIN CONTRABAND?

News for the week

Telecommunications security professionals, members of law enforcement organizations and public prosecutors may not be able to shut down computer data thieves if new advocates of hackers rights have their way. Support for Legion of Doom suspects developed as reporters following developments in the highly successful Operation Sun Devil crackdown listened to only one side--the hackers.

Apparently, the press got interested in digging into whether suspects' civil rights had been denied after Lotus 123 developer Mitch Kapor was approached by five attorneys complaining of overzealous enforcement tactics in Operation Sun Devil, the largest operation of its kind ever.

Kapor, who is president of On Technology, Inc., of Cambridge, Mass., responded by contributing $200,000 to a defense fund for alleged technopunks. Next, he formed the Institute for Computing Freedom, an apparent foundation for hackers' rights.

The highly respected American Civil Liberties Union got into the act after news reports of possible rights abuses surfaced in the Washington Post and New York Times. The result was that a June 9 Congressional Judicial Committee hearing on Caller ID matters was postponed so that hackers' rights can be addressed.

Rest assured that the hacker suspects will have highly articulate advocates at the hearing later this summer.

Assorted Numbers With Abuse On Them

- (800)225-0312 (PBX), two nine-digit codes; (800)535-4991, one five-digit code; (800)336-7800, one 10-digit code; (800)245-6332, three 10-digit codes; (800)843-3313, three six-digit codes; (800)327-9488, one 13-digit code; (800)248-8034, one six-digit code; (800)345-0017, six nine-digit codes; (800)962-4656, one six-digit code; Pheatures Newsline: (800)255-9679, box 262 and (800)877-5599, a number with high abuse by the hacker ORBID. (800)748-0375, Phillips Fibers, Inc.; (800)444-1333, (800)633-8256, (800)873-5669, (800)877-3444, (800)845-8856, (800)433-4467, (800)873-5666, (800)633-4102 and (800)535-6246.

- "Hackers are going after a carrier": (800)986-XXXX.

- PBX: (800)223-5517.

- 950-0511, three six-digit codes; 950-1022.

- Diverter: (800)422-7777.

- (313)980, plus the following mailboxes: Black Wizard, 8730; Mystic, 7760; Dark Side, 7558 and 7240; Phreak, 9077; Macho Man, 6846; Crocodile Posse, 4586; Sid, 7095 (personal box), 9157 and 5610 (Sid's codeline); Violator, 8839;5457 (codeline).

THIS USEFUL NEWSLETTER IS AVAILABLE THROUGH THE COMMUNICATIONS FRAUD CONTROL ASSOCIATION, PO BOX 23891, WASHINGTON, DC 20026 OR 7921 JONES BRANCH DRIVE, SUITE 300, MCLEAN, VA 22102. (703) 848-9768

(continued from page 39)

shiny new penny with all of this garbage — by far the most valuable thing in the envelope.

***

By calling 1-900-USA-BUSH, you can delude yourself into thinking that you've sent a fax to the president! According to the telecommunications magazine TE&M, which really should know better, this service "provides every American citizen a personal 'hotline' to the president of the United States, George Bush, to comment on issues or pending legislation." Each call costs $7.95. The plus side is that you actually get something in the mail: a copy of the fax with a stamp of the president's signature. By the way, if someone can provide us with the *real* White House fax number, we'll print it. Your chances of actually having your message read by someone will be much greater and your phone bill will be much lower.

***

MCI has begun offering nationwide 900 service and seems determined to avoid the pitfalls of its predecessors. New 900 services must provide proof that their programs don't violate any regulations or telephone company policies. Advertising will be examined to make sure it's not deceptive. And MCI will insist that callers be notified of the price of the service and given enough time to hang up if they're not interested. Anything child-oriented cannot cost more than $4 total. And all adult-oriented services have to be on the same prefix so they can be easily blocked.

***

British Telecom now offers a service for its troops in the Persian Gulf to call home more easily. It's called "Desert Direct" and allows soldiers to reverse the charges for less than the direct dial rate. A time limit of 10 minutes is enforced to allow as many people as possible to use it. Meanwhile, Military Communications Corp. of Eden Prairie, Minnesota has opened three Phonecenters in Saudi Arabia, each of which has 144 phones. They will be able to carry more than 30,000 outbound credit card and collect calls every day. Military Communications Corp. also owns Phonecenters on military bases throughout the United States. And AT&T has set up a toll-free number for families that are having trouble paying their phone bill because of calls from Saudi Arabia (800-323-HELP).

***

In light of the recent AT&T failures where massive amounts of callers are unable to get through to 800 or 900 numbers because of computer problems or cable cuts, the geniuses in marketing have come up with a solution. "Alternate Number Translation" would store the customer's 800 or 900 number into a backup database. Then when AT&T's system fails yet again, AT&T would use the backup database to complete the calls. For $500 per number per month (plus a $500 setup fee), AT&T will try to keep its failures from affecting you. We'll be trying to find out the names and numbers of everyone who agreed to these terms so we can try to get some free money too.

***

If you're interested in a worthwhile 800 service, Cable and Wireless seems to have the best low-cost system. For $10 a month plus calls, you can have your own 800 number. For $20 a month plus calls, you can have a *programmable* 800 number. This is a great service for those of us who move around. Simply call a special 800 number, enter your code, and you can program your 800 number to forward anywhere in the country! The cost of the calls themselves are higher than directly dialed calls, but not by an obscene amount and far less than calling card calls. We think this is very useful for those of us with imaginations. Imagine what would happen if some rich entrepreneur-type set up his/her 800 number to forward to the White House! All of a sudden, every poor person in America would be able to get their opinion heard. (The White House doesn't accept collect calls nor provide any 800 service.) Technology in the hands of imaginative people can do wonderful things.

***

developments

Here's a reason to stay off the phone. Remember Telesphere, one of those companies that occasionally shows up on your phone bill asking for huge amounts of money for 900 numbers? Remember NTS, one of those companies that occasionally shows up on your phone bill asking for huge amounts of money for operator-assisted calls? They are now one.

***

"NYNEX is more than a family of companies, it is a family of people. We must be an ethical family. The only behavior that is appropriate for our businesses and for each of us, is behavior that meets our high ethical standards. There can be no compromise." So begins an internal memo from NYNEX encouraging its employees to rat on each other by calling 800-473-TALK from 9 am to 7 pm. After that they can leave a message on their hackable voice mail system at the same number.

***

Kevin Mitnick made news again when he was barred from attending a computer symposium in Las Vegas last autumn. The Digital Equipment Computer User Society says it never had a known hacker attempt to register for one of its symposiums before. Their hysteria fits right in with the media and government portrayal of Mitnick as the biggest threat known to computers. In retrospect, the crimes Mitnick was convicted of seem grossly out of proportion to the sentence he received: a year in prison, some of which was served in solitary confinement and without access to a telephone. This unfairness, along with Digital's panic at his appearance, will hopefully be seen one day as the absurd reaction of short-sighted individuals who let fear prevail over common sense.

***

Hungary is the first Eastern European country to get 800 service to the United States.... Ameritech, NYNEX, and BellSouth have all been granted permission to offer electronic telephone directories. It could be a great service if the cost is kept to a minimum.... Southwestern Bell is offering an electronic directory service called Directline Custom for large businesses. Each screen of information costs 9.2 cents and the charge for a user ID is $8.80. Oh yes, there's a one-time establishment fee of $4152. The service is located in St. Louis and is accessible via dial-up. AT&T will soon be offering the same service and it will be called "AT&T Find America".... Despite a lot of publicity, Pacific Bell's Message Center service can't seem to stop crashing. For the second time in a week in December, the "alternative to an answering machine" went down causing thousands of people to lose their messages. For four hours in the middle of the day, users couldn't access the system at all. Pacific Bell is still proud of the service, saying it's only failed a few times "not counting brief 2 am to 3 am kinds of outages". We don't know where they're coming from but we want no part of an "answering machine" that goes down for maintenance whenever it feels like it.... BellSouth claims to have become the first of the regional Bell companies to be completely electronic. No more crossbars, no more steps.... According to The New York Times, Bulgaria has become the breeding ground of "the world's most lethal computer viruses". Not only do they produce the most viruses, says a virus expert, they produce the best. Why is this? Apparently, a generation of Bulgarians has learned how to program but has no way of using their skills in society.... New York Telephone will soon be testing a "debit" card at New York City payphones. Money will be taken out of your bank account as you talk.

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

DEFENDING HACKING

(continued from page 35)

have little or no understanding of what hacking is? Yes. Instead of being frightened by tall tales of hackers invading your privacy and taking over satellite transmissions and shutting down emergency phone systems, etc., I'm scared shitless over the *fact* that the government can kick my door in and take away my beloved computer because one day I called a bulletin board system that happened to be under surveillance for some random reason, or someone uploaded some sort of file to my bulletin board that I had no knowledge of. This can and has happened to innocent, unsuspecting people whose only crime was wanting to communicate with other computer users or download a public domain game.

Scenario: Joe Computeruser calls "The Gates of Eliteness BBS" one day hoping to get help on how to use his new spreadsheet package that he paid a large and legal sum of money for. He applies for an account and, as a result, his real name, age, address, and phone number (information that is required to gain access) are now stored in the BBS's user files. The sysop, Mr. Cool Joe Hacker, did something viciously maligned and has come under the scrutiny of the U.S. Government. His computer and all his files (and TV's, stereos, lamps, etc.) are confiscated, including the personal information of Joe Computeruser and countless other people who have accounts on the system. Joe Computeruser is now implicated in the investigation for collaborating in Mr. Cool Joe Hacker's exploits, along with the rest of the users on his BBS system, and is put under surveillance, even though he was calling for a most wholesome and legitimate reason. You don't think so, huh? Well, ignorance is bliss.

The government needs watching, not hackers. If hackers led the world, there wouldn't be half a million American troops in Saudi Arabia. Hackers don't send your sons and daughters to their deaths. The U.S. government does. While I cannot totally say "do not fear the hacker", I can say "fear the government".

After all is said and done, there is a limit. If a system exists that houses information, and you were not meant to be able to peruse that information then you do not have a constitutional right to be inside that system. But that's not to say that you won't go ahead and try to get into that system anyway. That's the choice you make, the rules of your game. There is such a thing as private property. That's one of the fundamental foundations our country is based upon. To use the argument that you have the right to be inside the computer systems of certain agencies gathering enormous amounts of information about you without your knowing, and to include in that argument that you have the right to be inside the computer systems of any private agency, company, etc. that houses information of any kind is not only entirely wrong, but stupid. But again, it all depends on the way the rules of your game are defined, the extent of your personal integrity, how screwed over you've ever been, and the way you look at life in general.

Since there will always be hackers, and there will always be those who think they have the right to be inside any system, the ultimate and unwavering responsibility lies on the owner of the system. If you don't make it secure enough, although you're not *asking* for someone to break into it (who would be?), you've got to realize that not everyone out there gives a shit, and by golly, if they want to hack into your system and they can, well then that's just what they're going to do. And that means that you overlooked something that you shouldn't have. That's life. That's the game.

If you enjoyed this issue, you may be interested in issues of the past. Move your eyes to the right for details.

HURRY UP

Time is starting to run out. 1991 is sure to contain lots of unpleasant things, but one of the worst will be a price increase for 2600 subscribers. We're not raising the price out of malice or because of some distant dictator. This is not a sneaky attempt to raise money for war bonds or terrorist activity. Simply put, we're increasing our price because our costs have gone up: postage, printing, and so on. The same old story. By renewing your subscription now, you can still take advantage of the old prices. Because next issue just won't be the same.

INDIVIDUAL SUBSCRIPTION

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

CORPORATE SUBSCRIPTION

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

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

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

BACK ISSUES (never out of date)

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

❑ 1988/$25 ❑ 1989/$25

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

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

TOTAL AMOUNT ENCLOSED: _____

internal organs

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