CONTENTS

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

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

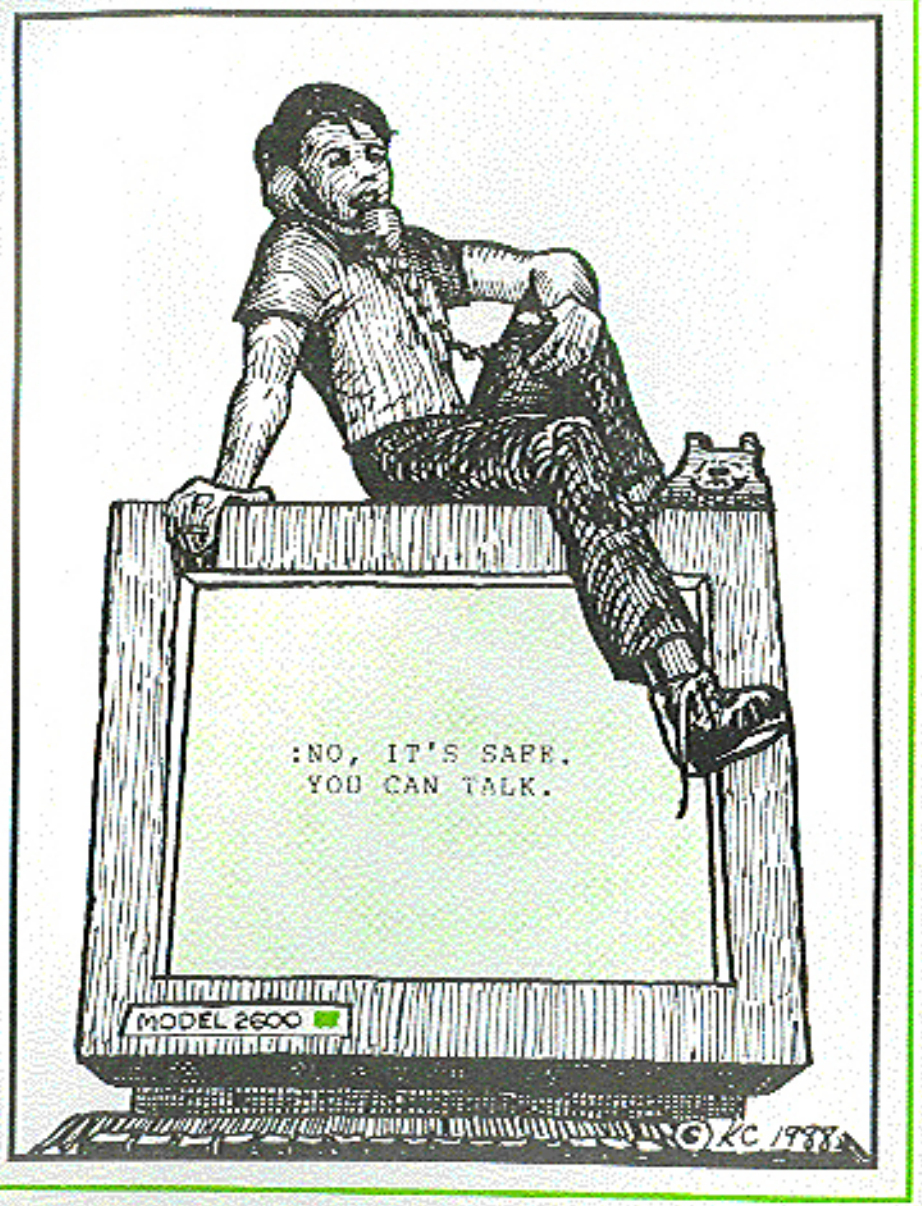
Forwarding and Address Correction Requested

DANGER:
MISSING LABEL

2600

The Hacker Quarterly

Volume 5, Number 1 Spring, 1988 $4



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

1984

AHOY!—an introduction to 2600. FBI GOES AFTER ADS HACKERS—FBI investigator unwittingly reveals tactics and recent activities. FLASH: LICA discusses GTE raids, AT&T credit cards, wireless phone trouble. THE TRUTH BEHIND THOSE 2600 NUMBERS—a [illegible] story. DATA: various White House [illegible]. HACKING ON TELENET—how to [illegible] Telenet use. ESS: ORWELL'S PROPHECY—the first in a series on the fun and dangers of ESS. FLASH: directory assistance changes, computer air-ban, AT&T credit cards, etc. SOME THOUGHTS ON GARBAGE PICKING—first of a series of trashing for valuable information as related to a discussion of crosstalk. DATA: COUNTRY CODES—every last country code for overseas dialing. THE CONSTITUTION OF A HACKER—a discussion of hacking. ALTERNATE LONG DISTANCE: MCI—history, systems, and services. FLASH: 313, Connecticut wiretaps, Sweden person numbers, etc. THE FIRST ATOMIC BOMB—an inside story on the event as related to our nation's phone system. DATA: ARPANET HOSTS—list of accessible hosts. WHOSE STRIKE WAS THAT ANYWAY?—a startling analysis of summer 83 phone strike. THE TROUBLE WITH TELEMAIL—discussion of GTE's irresponsibility in protecting their system. FLASH: AT&T credit cards, portable phones, 414's plead, etc. A TRUE SAGA OF TELECONFERENCING—what can happen on a teleconference. DATA: MCI ACCESS NUMBERS—DIALUPS FOR MCI MAIL. PHONE BOOK COLLAGE #1—our artistic heritage in phone book designs. THE SIMPLE PLEASURES OF A STEP OFFICE—discussion of ins and outs of antiquated phone systems. IBM'S AUDIO DISTRIBUTION SYSTEM—using voice messaging technology. FLASH: 414 sentencing, equal access, bank record privacy, etc. THE WOES OF HAVING A SMALL TIME RURAL PHONE COMPANY—a true story. DATA: AVAILABLE NETWORKS ON THE DEFENSE DATA NETWORK—a list including base addresses. EASYLINK ACCESS NUMBERS. ARPANET HOPPING: AMERICA'S NEWEST PASTIME—how it works and tips for its use. ELECTRONIC SWITCHING ADVANCES—some of the possible services and drawbacks. FLASH: Directory assistance charges, 2600 writer indicted, demise of E-COM, etc. THE DARK AND TRAGIC SIDE OF THE GREAT BREAK UP—a frank discussion. LETTERS: Sprint problems, 516-780 an XY area, etc. DATA: E-COM ACCESS NUMBERS—dial ups for the now-defunct service. NY TELEPHONE "LETTER OF DOOM"—a copy of a law enforcement monitoring notice. "LOOK OUT, HE'S GOT A COMPUTER!"—a defense of the hacker viewpoint. MCI MAIL: THE ADVENTURE CONTINUES—an analysis of the well-known faulty E-mail system. FLASH: computerized meter maid, blue box arrests, anti-hack legislation. INTRODUCING THE CLEAR BOX—[illegible] pay phone device. LETTERS: new switching equipment, 99 scanning, [illegible] operator story, etc. SPECIAL REPORT: TRW—BIG BUSINESS IS WATCHING YOU—how to use TRW, and an assessment of the potential of this system. BUT HOW DOES IT WORK?—an introductory explanation of the phone system, wiring, voltages, black boxes, ring, etc. PRIVACY LOST—a review of David Burnham's book "The Rise of the Computer State". BE NICE TO YOUR TELCO—how individuals are abusing their telcos. FLASH: Big Brother in Miami, NASA computer breaks in, computer export controls, 800 directories. LETTERS: phone scramblers, page numbers, hacker's book, etc. DATA: CNA NUMBERS—list of CNAs. A HACKER'S GUIDE TO AN AREA CODE—a simple scheme to help "map out" exchanges in your area. HISTORY OF BRITISH PHREAKING—an account of the history and techniques. MORE ON TRASHING—what to look for, where to go, how to act. A FRIEND IN HIGH PLACES—story of a friendly operator. FLASH: NSA insecurity, hacker caught, private directories. LETTERS: phone loop, WATS, TAP, etc. DATA: A NON-COPYRIGHTED DIRECTORY. NY TELEPHONE "BIG BROTHER" LETTERS—touch tone without permission, etc. GETTING CAUGHT: HACKER'S VIEW—a story of the personal effects of hacking. VITAL INGREDIENTS—what makes the phones work: operators, switching. FLASH: NSA wants better phones, crime computer victim, wiretap loopholes, 911 attacker caught. LETTERS: BBS discussion, Comsec Letter, Computer Crime Data, others. DATA: NY TELEPHONE SECURITY NUMBERS. MCI ANECDOTE—ads, vulgarisms, MCI chairman profile. PHONE BOOK COLLAGE #2. EXPLORING CAVES IN TRAVELNET—an interesting extender explained. FUN WITH FORTRESS FONES—what a pay phone does, how people beat them. FLASH: SS computer foul ups, Airfone, wiretaps, 815, pay phone wars. LETTERS: book list, silver boxing, another hacker's view. DATA: IC'S AND CARRIER IDENTIFICATION CODES—guide to 950 exchange. MCI MAIL "TROUBLE LETTER"—the harassment begins. A TIME FOR REFLECTION—the year in review. MCI MAIL AND EASYLINK—electronic mail horror stories. THE SCARIEST NUMBER IN THE WORLD—true story. FLASH: campaign computer, Pentagon by phone, students bop computer, a [illegible], [illegible] phone upgrade. SURVEY—reader survey responses. SOME, BUT NOT ALL ELECTRONIC MAIL SYSTEMS—list and price comparisons plus voice messaging companies. REACH OUT AND GOOSE SOMEONE—list of many unique dial-it numbers.

1985

THOSE HORRIBLE HACKERS STRIKE AGAIN—analysis of Newsweek incident. WIRETAPPING AND DIVESTITURE—a lineman discusses these topics. GETTING IN THE BACK DOOR—a guide to some popular operating systems including TOPS 10, TOPS 20, and UNIX. 2600 INFORMATION BUREAU: our phone bill, our thanks, and other notices. FLASH: IRS and telco data, GE-SCO, KAK computer. LETTERS: BBS rights, Easylink, Canada loops, international phreak day. BITNET TOPOLOGY—a schematic of the Bitnet. THE THEORY OF "BLUE BOXING"—history, future, and how they are used. TRASHING ALASKA STYLE—a real trashing adventure story. SURFING THE COSMOS—a beginner's guide to COSMOS, Bell's computer program. FLASH: phreak roundups, real TRW crime, 2600 BBS, 800 dial. LETTERS: Bell problems, telco discounts, marine calling, many questions. 2600 INFORMATION BUREAU—an extensive list of useful long distance jargon. NAZI BBS A CHALLENGE TO HACKERS—the role of the hacker. ARE YOU A PHREAK???—humourous review of phreaking. HOW TO GET INTO A C.O.—a tour of a central office. FLASH: custom calling, Korean pay phones, hacker coke machine, IRS computer screw ups. LETTERS: reading list, tracing and law enforcement, UNIX info, NSA phone #. 2600 INFORMATION BUREAU—interesting phone numbers, how to dial a telephone, New York Tel message, CNA LIST, NSA CIPHER DISK. WHAT A WHITE BOX CAN DO—how to build and the uses of a portable touch-tone generator. A PHONE PHREAK SCORES—another successful social engineering story. HACKING PACKARD—useful information about the HP2000. FLASH: talking clock, computers for communists, robot kills man, war games, silver pages. LETTERS: Ten Tom picks, secure telephones and cryptography. 2600 INFORMATION BUREAU—MILNET hosts by location. PEOPLE EXPRESS TO BE HACKED TO PIECES—a look at People's new anonymous reservation service. HOW TO RUN A SUCCESSFUL TELECONFERENCE—complete guide to Alliance Teleconferencing Service. FLASH: hacker bust, police hacker, Reagan doesn't dial kids, dial-a-directory. LETTERS: computer networks, silver boxes, 950, rotary, tracing. 2600 INFORMATION BUREAU—Alliance Teleconferencing material. INTERESTING PHONE NUMBERS: UNBELIEVABLE ADVERTISEMENT. GUIDE TO THE ISRAELI PHONE SYSTEM. SHERWOOD FOREST SHUT DOWN BY SECRET SERVICE. SOME WORDS ON HACKER MORALITY. OUT OF THE INNER CIRCLE REVIEWED—an ex-hacker's new book. FLASH: who invented the phone, porno phone, wiretap award, AT&T computer woes. LETTERS: information charges, AT&T cutoff, marine calling. 2600 INFORMATION BUREAU—800 prefixes by state. SYSTEMATICALLY SPEAKING: goodbye to meter readers, Thai phone books, tracking devices, TINA, "Call Me" Card. FROM SHERWOOD FOREST: INTRO TO HACKING—what to do and not to do. INTERESTING THINGS TO DO ON A DEC-20—how to use various commands and some things to look for. BANKING FROM YOUR TERMINAL: A LOOK AT PRONTO—Electronic banking, how it works with a focus on Chemical's system. FLASH: 92 billion error, ITT crackdown, monitoring. 2600 INFORMATION BUREAU—Milnet TAC dialups by location. SYSTEMATICALLY SPEAKING: MCI goes optical, 100% ESS, GTE bigger than AT&T. SEIZED! 2600 BULLETIN BOARD IS IMPLICATED IN RAID ON JERSEY HACKERS—an accurate account of the Private Sector BBS. COMMENTARY: THE THREAT TO US ALL—what BBS seizures mean. FLASH: 2600 a hacking victim, Middlesex Courthouse. MOVING SATELLITES: WHAT WAS REALLY GOING ON?—point by point correction of New Jersey prosecutors' fallacious charges. WHY COMPUTERS GET SNATCHED—why law enforcement seizes equipment. SOME IMPORTANT QUESTIONS TO ASK—provocative questions about these events. HOW CAN SYSOPS PROTECT THEMSELVES?. A GUIDE TO VMS—how to use DEC's VAX operating system. THE INFINITY TRANSMITTER—an old bug explained. REACHING OUT ON YOUR OWN—blue boxing verification. PURSUIT FOR PEOPLE—GTE Telenet's computer to computer link up service. FLASH: phone-in registration, 800 word numbers, war game socks, hacker [illegible]. 2600 INFORMATION BUREAU—Telenet directory of interesting addresses. SYSTEMATICALLY SPEAKING: Dick Tracy toys, computer directory assistance, Bell propaganda films, European standardizing [illegible]. MANY FAMILIAR TONES. AND THEY CALL US CROOKS?—story of a phone phreak who can't get his expenses. AN INTERESTING DIVERSION—call diverters and how they are abused. MORE INFO ON VMS—second installment of an in-depth guide to VMS. FLASH—computer elections, big phone bill, Navy phreaks, phone booth [illegible]. LETTERS: BBS suggestion, colleges are a gold mine, recommended reading. 2600 INFORMATION BUREAU—Blue Box plans. THE NEW AT&T HOSTAGE PHONE—unbelievable ad. SYSTEMATICALLY SPEAKING: hackers scare businesses, DuPont bypasses telco, computer campaign info, phone computers, divestiture woes. RSTS: A TRICK OR TWO—some aspects of this operating system. THE SECRET REVEALED—the problem with GTE's GTD-5 switch. HISTORY OF ESS. EQUAL ACCESS MAY NOT BE "TOTAL" TO MODEMS—some problems that may arise. FLASH: columnist attacks AT&T, feds dial it too much, little town phones, Springsteen mania. LETTERS: some advice, CIC's and free calls, British phreak, blue boxing gone? CHASE BANK IS CRACKED. 2600 INFORMATION BUREAU—many interesting test numbers. SYSTEMATICALLY SPEAKING: avoid phones in storms, rural unequal access, police cellular phones, toll free from errors, AT&T to read e-mail. OUR WISHES FOR '86 AND BEYOND—some of what we'd like to see in the future. FUN WITH COSMOS—how to interpret and use parts of the phone company computers. FLASH: French phones, radar banter, Cryphone. SURVEY—reader survey responses. 2600 INFORMATION BUREAU—BBS numbers. SYSTEMATICALLY SPEAKING: AT&T e-mail, German phones, super pay phone.

(continued on inside back cover)

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

Never before have so many pages been printed in a hacker publication. There are so many topics to discuss that are relevant to our "cause". In this issue, you'll find pieces about disastrous telephone systems, the effects of becoming dependent on computers, ways of eavesdropping on telephone calls in such a way as to be completely undetectable, additions to our previous articles on IBM computer systems, and an interesting look at the world of phone phreaks and computer hackers which contrasts with the way we actually see ourselves. Plus all kinds of numbers, codes, displays, and reproductions that ought to make it all more interesting.

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

(continued on page 8)

STAFFBOX

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Bobby Arwatt

Production
Mike DeVoursney

Cover Art
Ken Copel

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

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

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

Copyright © 1988, 2600 Enterprises Inc.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available for 1984, 1985, 1986, 1987 at $25 per year, $30 per year overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO: 2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO: 2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
2600 Office Line: 516-751-2600
BBS #1 (OSUNY): 914-725-4060
BBS #2 (CENTRAL OFFICE): 914-234-3260
BBS #3 402-564-4518
USENET ADDRESS: 2600@dasys1.UUCP
ARPANET ADDRESS: phri!dasys1!2600@nyu

monitoring phone calls with a TVRO

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

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

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

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

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

Some years ago it was pointed out that 68 percent of long distance telephone trunks went by ground based microwave. And while the long distance carriers have been working (under some pressure from the NSA and White House) to convert these circuits to optical fibers or at least coaxial cable there are still many routes that use microwave or satellite hops. I don't know an exact figure but I think it would be reasonable to guess that at least 40-50 percent of long distance trunks include a microwave or satellite hop. And some 75 percent (approximately) of long haul microwave relays use the 3.7-4.2 Ghz band which is readily receivable by a TVRO.

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

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

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

This vulnerability has been well known in security circles for many years, but as the number of TVRO systems has increased to over a million, the problem assumes a somewhat different perspective. In 1976 Mitre estimated that it would cost $50,000+ to intercept microwave telephone calls, and would require a 10 foot dish. In that era a 10 foot dish would attract much attention. Today one can buy a TVRO system with a 75k LNA and an 8-12 foot dish for $1000-$1500, and almost nobody will give the system a second glance as TVRO's are commonplace. A 75k LNA beats the 10-12 db noise figure receiver that Mitre based its calculations on by a very substantial amount. And the current generation of computer controllable general coverage SSB receivers are much cheaper demultiplexing devices than the synthesizer and selective voltmeter that seemed necessary in 1976.

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

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

Background

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

Multi Channel systems

1. FDMA-PSK-TDM-PCM.

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

2. TDMA-PSK-TDM-PCM.

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

3. FDMA-FM-FDM-SSB.

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

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

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

Single channel systems

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

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

monitoring phone calls

(continued from previous page)

converter. Easy for private individuals to intercept.

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

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

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

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

On FM-FDM-SSB

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

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

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

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

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

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

with a TVRO

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

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

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

On PSK TDM

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

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

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

(continued on next page)

monitoring with TVRO

(continued from previous page)

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

TDMA-PSK-TDM-PCM signals are much more complex than most FDMA-PSK-TDM-PCM signals. This is natural since all traffic is transmitted by having each station on the network transmit a burst of very high speed (tens of mb/s) data in an assigned time slot round robin fashion. Included in the burst is all of the traffic that station has with every other station on the network. Every other station monitors all the bursts from stations it is in communication with and picks out the channels that correspond to its incoming traffic. In many such systems, burst lengths and time slots are dynamically assigned by a master ground station computer as calls are set up and terminated. Each station is capable of receiving and decoding the bursts transmitted by every other station it talks to, so if the channels are not encrypted it could monitor much of or all the traffic going through the transponder.

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

(continued from page 3)

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

We've also been getting a lot of positive press response in the past couple of months, including a spot on a most incredible television program, Network 7 on England's Channel 4. This program ought to be seen by every reporter in this country who wants to do a story on computer hacking. Instead of looking at the "problem" of hackers and what they could be doing to you in the same way we've seen hundreds of times already, the producers of this program looked at the positive aspects—the adventure, imagination, and intelligence involved. It wasn't just that they gave hackers a positive image—they used their brains and created a different way of viewing a topic. That's something we can all use a bit more of. Our thanks to John Drake for making this possible.

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

VM/CMS CORRECTIONS

by VM Guru

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

Comments on Part 1

A few general points to start:

- There are two types of VM systems. The first is (usually) fairly small, typically on an IBM 4331, 4341, 4361, or 4381. They are generally unmodified and tend to use the IBM default names for system userids and often passwords. Unless you work there, cracking these systems will be difficult because they usually have no data connections to the outside world.
- The other general class of VM system is fairly large, running on a CPU such as a 3081 or 3090. These systems are often modified, both to provide function and security. Some of these mods are described below. Many of these mods are passed around at conferences, workshops, or by a conferencing (BBS) system (which will remain nameless).
- The VM system lends itself to modification because most of the source code is distributed with it. For a long time, IBM treated VM as an orphan stepchild and tried to bury it. The users wouldn't let them, and IBM finally recognized it as a going system. VM has now passed through eleven releases, and the twelfth has been announced.
- VM (or CP, the two terms are often used interchangeably) is not an "operating system" in the usual sense of the term. You can't run "jobs" (processes) under it. Rather, you run operating systems under it and each user runs an operating system. Each logged on user gets a "virtual machine" to run his operating system in. Each virtual machine has a CPU, memory (storage), disks, tapes, and unit record (card or printer) devices. Some of these correspond to real devices, and others are virtual. A virtual disk can be represented by a small portion of a real disk. Unit record is usually "spooled" to/from disk. Most systems these days have no real card equipment, and the virtual card equipment allows data to be passed between users as "card images" (80 byte records). All functions that would be buttons, dials, or lights on a real machine are represented by query or set commands to CP in a virtual machine.
- CMS is a single user interactive operating system that is tailored to run very well under VM.
- Other operating systems that are often run under VM are batch systems such as MVS, DOS/VSE, or VS1. These can run both batch or interactive systems such as TSO, CICS, ICCF, or others. (See the discussion of DIAL below.) A second copy of VM can run under VM, and this is often used to test modifications and new releases. Basically, anything that can be run on the real hardware can be run under VM in a virtual machine.
- VM natively supports three types of terminal. These are 3270 display (CRT, video) terminals (in many flavors), 2741/3767 (typewriter-like terminals), and ASCII terminals such as the IBM 3101, TTY's, and ASCII CRT's (such as the VT-100) in line mode. A PC that emulates one of these can also be used. To support ASCII CRT's in full screen, a protocol converter is needed. Both hardware and software versions of protocol converters are available. These make the ASCII CRT look to the VM system as if it were a 3270 terminal. Various escape sequences are used to simulate 3270 functions that the ASCII CRT may not have.

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

- While it was late in coming, VM has had online help for some time. It's slow, it's clumsy, but it's there. Enter "HELP HELP" to get started.
- While the system is somewhat cumbersome, that's mainly because of the wealth of functions available. If you found it hard to learn, then either you didn't have the manuals that are needed, or you had a poor teacher (or

(continued on next page)

VM/CMS CORRECTIONS

(continued from previous page)

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

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

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

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

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

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

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

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

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

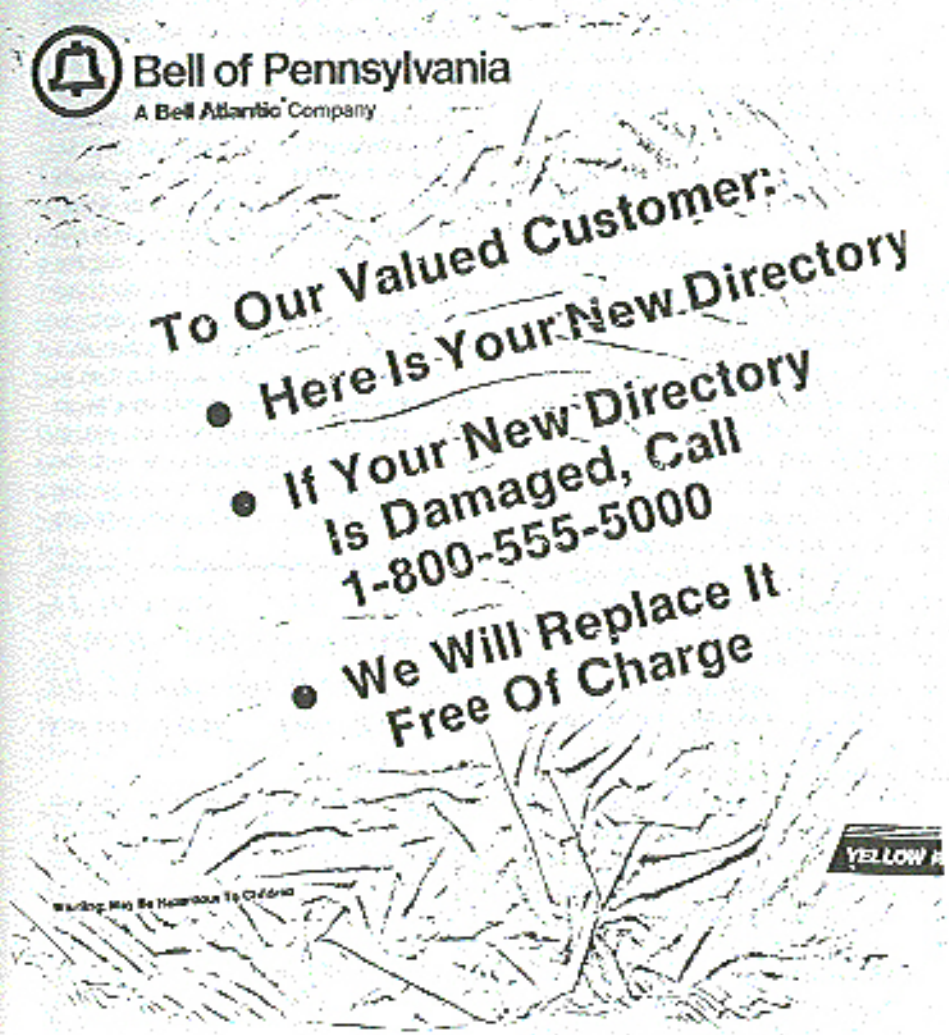
• The reason that "BONEHEAD" (to use Lex's example) is "not valid before logon" is that because of the extensibility of VM/CMS, BONEHEAD could very possibly be a valid command, either local to one user, a group of users, or systemwide.

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

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

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

(continued on page 12)



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

(continued from page 10)

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

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

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

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

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

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

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

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

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

CORRECTIONS

Comments on Part 2

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

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

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

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

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

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

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

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

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

7. Search for a nucleus resident command.

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

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

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

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

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

13. Search for a CP command.

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

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

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

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

(continued on next page)

VM/CMS CORRECTIONS

(continued from previous page)

is not processed by CMS.

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

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

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

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

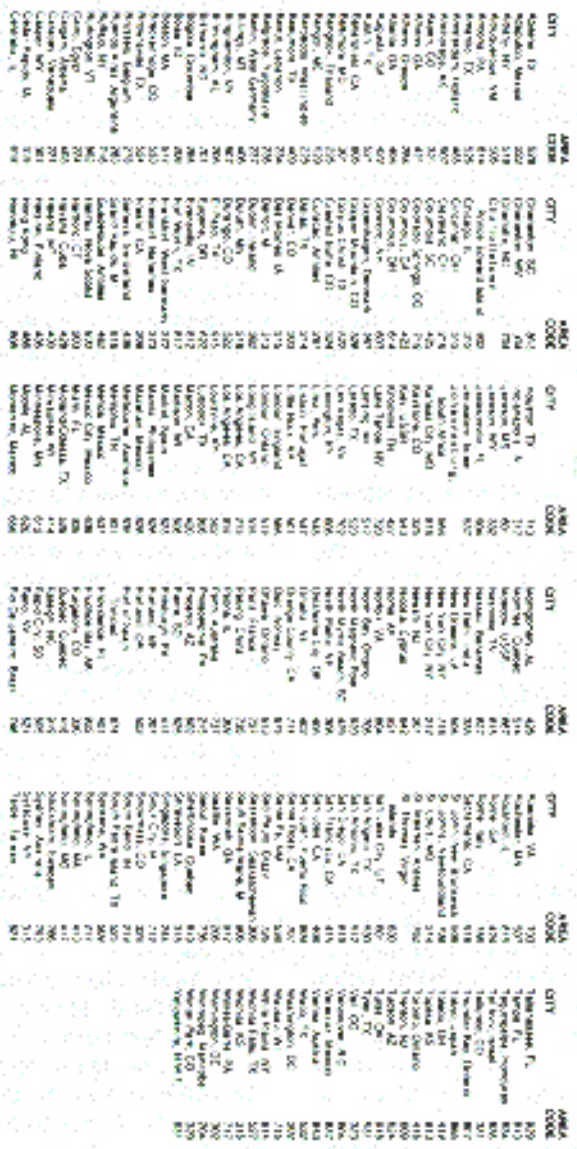
```
DASD 130 CP OWNED VMIPOE 0044
DASD 154 CP SYSTEM SYSWK1 0001
DASD 249 ATTACH TO VSEIPO 246
```

What this listing shows is that VMIPOE on real address 130, is "OWNED" by CP (i.e., it contains one or more system data areas), and the currently logged on users have 44 minidisks on this pack. This can be 44 users all with the same minidisk, 44 different minidisks, or some combination. SYSWK1 is on 154, has no system data areas, and at the moment is in use by one user with one minidisk. Real address 249 is attached (dedicated) to user VSEIPO as his virtual address 246.

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

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

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



THESE ARE WEATHERTRAK CODES. WHEN DIALING THE WEATHERTRAK SERVICE, SIMPLY ENTER ONE OF THESE TO RECEIVE THE FORECAST FOR THAT PART OF THE WORLD. WE UNDERSTAND THERE ARE SOME HIDDEN CODES AS WELL. THE NEW YORK ACCESS NUMBER IS (212) 355-1212. TO FIND OUT THE NUMBER NEAREST YOU, CALL 800-247-3282 OR (214) 556-1122.

An Interpretation of Computer Hacking

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

by Captain Zap

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

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

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

Telecommunications and Fraud

The beginning of the formal underground phone network started in 1971 with the formation of the newsletter entitled "YIPL" or Youth International Party Line. This newsletter was structured with information on how the phone company equipment would work and ways to defeat it. This was also seen as a protest against the Vietnam war and the federal tax that was placed on phone service to help pay for the war.

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

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

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

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

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

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

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

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

Black: does not allow the connection of billing circuits to call. Must be used on called party's line. This is only usable on older switches such as step by step or #2 or #5 Crossbar.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

An example of a simple "Wargames" program

(continued on next page)

(continued from previous page)

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

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

(See WARGAMES listing on page 20)

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

Hacker Communications and Bulletin Boards

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

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

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

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

But this writer's opinion about the attack is that it was very successful showing the ability of certain persons who were able to shut down some of the phone service in the city. If such actions can be performed by persons who do not have inside information or access to the facilities, then it is a very real situation. Such attacks can be placed to a series of phone lines or just one. Other attacks have involved the reprogramming of Bell System switches, changing the destination of 800 toll-free calls to other locations, or ringing a vast number of phones at the same time.

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

Bulletin Board Systems

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

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

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

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

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

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

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

But the problem is twofold: the user must be held accountable for his actions and the owners must secure their machines with a reasonable amount of security.

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

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

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

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

(continued on next page)

The Hacker Threat

(continued from previous page)

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

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

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

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

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

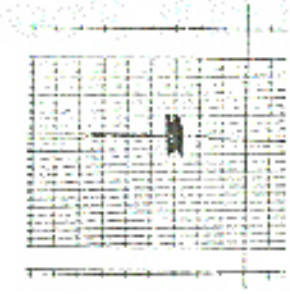



FIGURE 1
Nickel

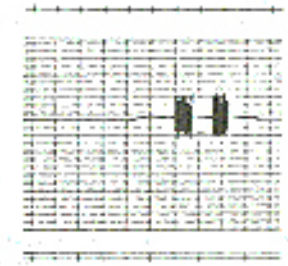


FIGURE 2
Dime

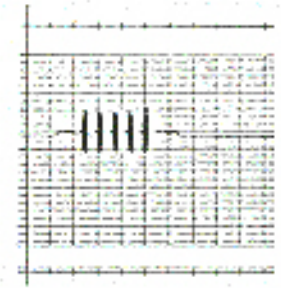
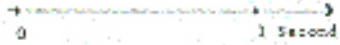


FIGURE 3
Quarter



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

FROM THE 2600 FILES

Bell Communications Research

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

August 21, 1955

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

Dear Mr. Paprcka:

I have completed examination of the floppy disk you brought to the Network Security Laboratory of Bell Communications Research, Red Bank, New Jersey on July 22, 1955. It relates to a New Jersey Bell investigation 2E-0038 involving Thomas Black, Private Sector bulletin board, Dover, New Jersey.

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

"Disk Number 041
THE CAT'S MEOW
CAT HACKER 3.71
SOUND PROGRAMS
M091"

The mark "TOP 7/22" also appeared on the label and at the time of my examination I added my mark "BCR-WHH 7/24/55."

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

On August 13, 1955, Patrolman Michael Grennier, South Plainfield, New Jersey, brought the following equipment to this laboratory:

An Apple IIe personal computer, SN 1303187 equipped with:
Novation Communications Module, 4105J
Hard Disk, XEBEC Mod. 9710P, SN 4-C794
Floppy Disk drives A2M0003, SN 1046016, and 1193212

Patrolman Grennier loaded the program "The Cat's Meow" from the 5 1/4 inch flexible disk into the computer and pressed the letter D on the keyboard to select the dial feature of the program. Progress of the program was observed on the monitor screen. The audio output was fed to signal analyzing equipment which included a Wilcom Model 7180 Tone Signaling FFT Analyzer and a Gould Digital Storage Oscilloscope, Model OS4C2C used with a Gould Brush 220 Recorder.

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

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

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

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

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

The flexible disk you brought is returned to you herewith.

Approximately 15 man-hours were required to perform this analysis.

Very truly yours,

Walter W. Heinze

Walter W. Heinze
Member of Technical Staff
Network Security

NVC-BCR23131-WWH-1j

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

SPRINGTIME LETTERS

More Secrets

Dear *2600*:

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

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

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

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

Doom

Encouraging Words

Dear *2600*:

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

A Friend in Texas

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

Still More Secrets

Dear *2600*:

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

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

The second system logs on saying it is "Marbles BBS" and operates like a regular (but weird) BBS. The following commands are available: A=answer call, B=??, C=??, D=??, E=e-mail, S=send letter, R=receive letter, M=make call, Q=quit. However, if you mess around with it enough, you'll get asked for a password. After getting through 15 passwords, 20 identification numbers, and 62 levels of access, the system tells you it is the "Military Operations Unit System" and then the Artificial Intelligence kicks in. Then from there if you were to tell it to "launch missile", it will ask you what type of missile, target, from where, etc. Then it will start a countdown. I stopped it before zero but I was wondering, could someone really launch the missiles? Isn't there a human factor involved?

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

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

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

A Very Special Number

Dear *2600*:

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

What a wonderful public service...

Tales of Hackers

Dear *2600*:

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

I found a goody in *An Introduction to*

Police suspect UT hacker stole long-distance codes

Cedar Park treasurer for Fire Department charged in fraud, theft

(continued on next page)

LETTERS OF THE SPRING

(continued from previous page)

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

```
REVENGE: PROCEDURE OPTIONS
(MAIN, TASK);
   WAIT(EVENT);
END REVENGE;
```

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

The Hooded Claw

Advice Wanted

Dear *2600*:

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

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

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

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

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

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

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

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

Of Phones and Politics

Dear *2600*:

The importance of the telephone in modern life became apparent in the recent New Hampshire Primary Debate of the Democratic party. The first question asked by the moderator was directed at Senator Paul Simon in reference to the Senator's proposal to put free telephones in the homes of those who could not afford them. He would place a two percent tax on long distance charges to pay for this program. Bruce Babbit attempted to discredit the proposal by challenging Simon to address the broader issue of the deficit. Gary Hart tried to ignore the subject altogether but Representative Albert Gore showed himself to be the most knowledgeable "telecom enthusiast" seeking the nomination by attacking the Reagan administration's policy of local "access fees" to subsidize long distance service for big businesses. Gore also stressed the need of making telephones affordable to the widest base of people possible. Telecom may be on the agenda, but we're waiting for a candidate who will support *2600*'s campaign against touch tone fees!

Skinhead Steve and The Boy

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

More on the 8038

Dear *2600*:

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

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

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

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

REMOB Hunting

Dear *2600*:

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

"The ultimate in phone spying is REMOB, remote observation. The phone company is said to have certain secret numbers—one is in Iowa—that can be used for listening in on other numbers. You call the REMOB number with a touch tone phone, then punch in two access codes and the phone number you want to tap—which can be anywhere in the country. The tapping is done by a sophisticated technique that does not create a telltale click, hum, or beep. It's all done automatically, without an operator, and anyone knowing the number and access codes can spy on anyone anywhere."

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

MH
Uniondale, NY

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

The Global Village

Dear *2600*:

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

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

(continued on next page)

LETTERS

(continued from previous page)

Foundation novel?

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

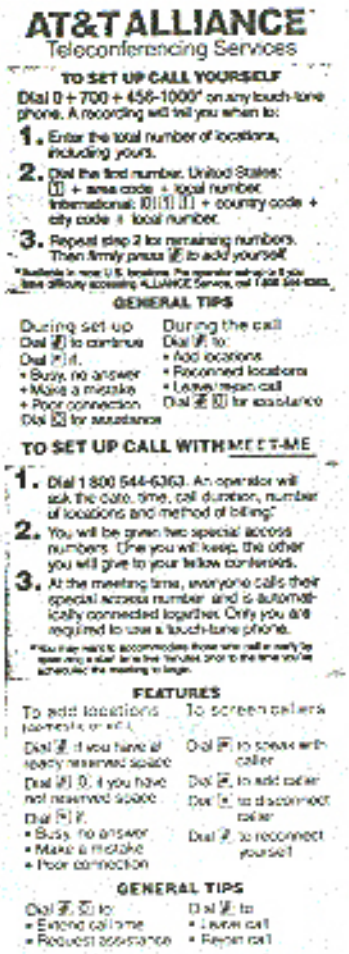
I hope the hackers and phreaks of the world are willing to write this much needed BBS software, because too many of us are kept apart by the telephone systems of our countries. For if we *really* wish to learn and finally *control*, we need common places where we can go to draw on and then expand our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

The NATO Association

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

***

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



AT&T ALLIANCE
Teleconferencing Services

TO SET UP CALL YOURSELF

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

1. Enter the total number of locations, including yours.
2. Dial the first number. United States: 1 + area code + local number. International: 011 + country code + city code + local number.
3. Repeat step 2 for remaining numbers. Then firmly press # to add yourself.

*Available in most U.S. locations. Pre-operator ratings in 5 min. New offices accessing ALLIANCE Service, call 1 800 344-0000.

GENERAL TIPS

During set up
Dial # to continue
Dial * if:
• Busy, no answer
• Make a mistake
• Poor connection
Dial 0 for assistance

During the call
Dial * to:
• Add locations
• Reconnect locations
• Leave/rejoin call
Dial # 0 for assistance

TO SET UP CALL WITH MEET-ME

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

*You may want to accommodate those who call in early by speaking with a clerk on the hour, minutes prior to the time you're scheduling the meeting to begin.

FEATURES

To add locations (owners or not)
Dial # if you have all legacy reserved spaces
Dial # 0, if you have not reserved spaces
Dial * if:
• Busy, no answer
• Make a mistake
• Poor connection

To screen callers
Dial * to speak with caller
Dial # to add caller
Dial 1 to disconnect caller
Dial # to reconnect yourself

GENERAL TIPS

Dial # 0 to:
• Extend call time
• Request assistance

Dial # to:
• Leave call
• Rejoin call

Attention Readers!

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

Remember, much of* 2600 *is written by YOU, our readers.

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

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

***2600* Editorial Dept.**
Box 99
Middle Island, NY 11953-0099
(516) 751-2600

RCI CORPORATION • 333 METRO PARK • ROCHESTER, NEW YORK 14623 • CUSTOMER SERVICE 1-800-828-2743

ACCOUNT NO. 002944 H

BILL DATE 02/26/88

PAYMENT DUE BY 03/25/88

PAY THIS AMOUNT 0.06

AMOUNT ENCLOSED

MAKE CHECK PAYABLE TO:

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

PLEASE RETURN THIS FORM WITH PAYMENT TO ENSURE PROPER CREDIT

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

ROLM Phone System

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

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

In The Beginning

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

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

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

In 1986, the university began installing a brand new phone system: the ROLM CBX II 9000. This would be the system to bring the campus into the information age, with useful features and high speed data capabilities.

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

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

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

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

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

Creates a Nightmare

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

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

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

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

a voice message system that is fairly flexible, but not a true replacement for one's own answering machine. Messages do get lost, mailboxes get full much faster than answering machine tapes, the system is easy to break into mainly due to three-digit default passwords and the fact that Phonemail provides a fairly complete listing of mailbox extensions after hearing a few stars from a touch tone phone. Plus the very simple fact that it just isn't tangible.

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

More Problems

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

It is true that the university

(continued on next page)

ROLM System Horrors

(continued from previous page)

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

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

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

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

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

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

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

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

(continued on page 34)

NEW DIALING INSTRUCTIONS

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

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

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

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

The University Hospital Main Switchboard Number will remain 495-8333. To call individual extensions (Direct Inward Dial Extensions) in the Health Sciences Center and University Hospital from off campus, dial "444-XXXX".

ROLM TELEPHONE SYSTEM USERS

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

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

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

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

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

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

International Calls—International calls can be placed without the assistance of the International Operator by dialing the call directly from a ROLM telephone:
Dial "9 + 011" + Country Code + City Code
(See International Code listings at end of directory)

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

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

HEALTH SCIENCES CENTER AND UNIVERSITY HOSPITAL

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

SL-1 SYSTEM USERS

On Campus Dialing

To call a "632" exchange on Main Campus:
Dial "9—632 + XXXX"
(These calls will be routed over tielines)

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

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

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

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

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

STUDENT DORMITORY CENTREX USERS

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

On Campus Dialing—

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

To call a "632" exchange on Main Campus:
Dial "122—2 + XXXX"
(If you have Unlimited Local Service:
Dial "9—632 + XXXX")

To call a "444" exchange in the HSC or Hospital:
Dial "122—4 + XXXX"
(If you have Unlimited Local Service:
Dial "9—444 + XXXX")

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

TELEPHONE REPAIRS FOR ROLM SYSTEM USERS

Between the hours of 8:00 a.m. and 5:00 p.m., all mechanical difficulties with your telephone should be reported to the Campus Repair Operator by dialing "5-0503" (cannot be dialed directly from off-campus). Please do not call telephone repair for installation, changes, or relocation of your telephone. Service of this kind must be ordered in writing through the Office of Communications Management Engineering, Suffolk Hall, Room 146, (246-3630). New Telephone Work Request Forms will be distributed in the near future.

TELEPHONE REPAIR FOR STUDENTS

The procedure for reporting telephone repairs for Residence Hall's (Centrex) telephones will remain the same. To report trouble on the telephone line, contact the New York Telephone Repair Bureau by dialing 9—611. Students who purchase their own telephone are responsible for its repair or replacement. If the telephone is leased from ATTIS, it may be dropped off at the nearest AT&T Phone Center for repair.

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

The ROLM College Campus

(continued from page 32)

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

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

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

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

Nightmares

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

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

Incomprehensible Bureaucratic Mess

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

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

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

Uselessness

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

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

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

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

(continued on next page)

ROLM System Horrors

(continued from previous page)

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

NOTE

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

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

As we said earlier, what's happened at Stony Brook is happening in other places. It represents something scary about our emerging technology. While great things are possible, so are big problems. And nothing will lead to disaster quicker than an unwillingness to prepare for those worst-case scenarios. It is vital not to be dependent on any form of technology because when it fails, you will be crippled. This is a very basic rule that is being followed less and less. How many of us have lost hours of work into thin air because of a computer glitch? Something as crude as a printed copy of our work could have saved us so much trouble. Crude backups must also exist on our new phone systems so that when they do unpredictable things, we'll be able to get access to the basics, like an outside dialtone.

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

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

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

HAPPENINGS

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

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

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

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

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

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

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

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

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

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

***

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

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

(continued on next page)

HAPPENINGS

(continued from previous page)

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

***

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

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

***

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

***

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

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

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

***

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

(continued on page 40)

State of Florida

COMMISSIONERS
KATIE NICHOLS, CHAIRMAN
THOMAS M. BEARD
GERALD L. GUNTER
JOHN T. HERNDON
MICHAEL McK. WILSON

DIVISION OF CONSUMER AFFAIRS
GEORGE B. HANNA, DIRECTOR
TOLL FREE 1-800-342-3552
(904) 488-7728

Public Service Commission

THIS IS A SPECIAL ADVISORY FROM THE FLORIDA PUBLIC SERVICE COMMISSION

PLEASE READ CAREFULLY!

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

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

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

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

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

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

Thank You,

George B. Hanna
Division of Consumer Affairs

FLETCHER BUILDING • 101 EAST GAINES STREET • TALLAHASSEE, FL 32399-0857
An Affirmative Action/Equal Opportunity Employer

HAPPENINGS

(continued from page 38)

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

***

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

***

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

***

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

OSUNY

2600 BBS #1

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

CALL TODAY!

914-725-4060

THE CENTRAL OFFICE

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

2600 BBS #2

914-234-3260

2600 Marketplace

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

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

QUALITY TAP REPRINTS. Complete set (#1-91) punched and bound. High quality copies with all special supplementals. $75/set, shipped UPS or USPS or 590/set shipped Federal Express. Money orders only, payable to Jeff. TZG, P.O. Box 1515, Columbus, NE 68601-1515.

WANTED: G-file "Better Homes and Blueboxing Part 2" by Mark Tabas. If anyone can provide a hard-copy, please send it to JRE, 1447 Graber Dr., Cleveland, OH 44107.

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

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

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

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

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

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.

FOR SALE: 8038 multi-purpose tone generator chips, prime quality $7.50 each ppd. Includes comprehensive applications data. Two chips will generate any dual tone format. These are no longer in production. Get 'em while they last. Bruce, P.O. Box 888, Stinson Beach, CA 94970.

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

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

Deadline for Summer issue: 5/31/88.

AT&T/BOC

The following is a list of routing codes used by AT&T and Bell Operating Companies (BOC) that you can blue box to. Most codes are used by dialing KP1NPA*XXX*ST, where XXX= the code, except where noted. There are notes attached after this list. Codes marked with a ? are unfamiliar to us.

000 Rate Quote System (RQS) (1)
001-005 Spare (2)
006-008 Reserved (3)
009 RQS
010 Reserved
011 International Origination Toll Center (IOTC) (15)
014 TWX Switching Plan (Canada) (2)
015-071 Spare
072-079 Reserved
080-081 Spare
082-087 Reserved
088 Spare
089 Reserved
090-099 Spare
100 Plant Test- balance termination
101 Plant Test- test board
102 Plant Test- Milliwatt tone (1004 Hz)
103 Plant Test- signaling test termination
104 Plant Test- 2-way transmission and noise test
105 Plant Test- Automatic Transmission Measuring System/Remote Office Test Line (ROTL)
106 Plant Test- OCSA loop transmission test
107 Plant Test- per meter generator
108 Plant Test- OCSA loop echo support maintenance
109 Plant Test- echo canceler test line
110-119 Operator Codes
115 Operator Leave Word
116 Inward DA
120 Network Emergency Center (2)
121 Inward Operator (3)
122 AT&T Readyline ISWATS (4)
123-130 Reserved
131 Directory Assistance
132-133 Reserved
134 IDDD for Equal Access (7)
135-140 Reserved
141 Rate and Route (10)
142-147 Reserved
148 Points not on an NPA- Hermosillo, Mexico (5)
149 Reserved
150 Cable Control (Satellite Avoidance)- Hawaii (5)
151 International Assistance
152-157 Reserved
158 Operator Assistance for Equal Access (7)
160 International Operator Center (IOC) (6)
161 Trunk Trouble Reporting
162-167 Reserved
168 Points not on an NPA- Grenada
169-170 Reserved
171 Points not on an NPA- Monterey, Mexico
172 Points not on an NPA- Dominican Republic, Puerto Rico, Virgin Islands. (Canada Only)
173 Reserved
174 Cable Control (Satellite Avoidance)- Caribbean
175 Reserved
176 Points not on an NPA- Mexicali, Mexico
177-178 Reserved
179 Points not on an NPA- Grenada
180 Points not on an NPA- Mexico Numbers
181 Toll Station
182 International Switching Center (ISC) White Plains, S (14)
183 ISC New York, SW24
184 ISC Pittsburgh
185 ISC Atlanta OIT
186 ISC Sacramento
187 ISC Denver\Sherman Oaks? (15)
188 ISC New York, 5450
189 Points not on an NPA- Mexico City, Mexico
190 Points not on an NPA Mexico Numbers
191 Conference loop around
191 AT&T Advanced 800 Intercept recording frames (4)
192 Reserved
193 Cable Control (Satellite Avoidance) Grenada
194 Points not on an NPA- Tijuana, Mexico
195 AT&T Advanced EIS (4)
196 AT&T International 800 (4)
197 Reserved
198 AT&T International City Service Center (ICSC)
199 Cable Control (Satellite Avoidance)- Alaska
199 AT&T USA Direct (4)

4 or 5 digit codes (8)

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

NOTES:

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

(continued on next page)

ROUTING CODES

AT&T/BOC

(continued from previous page)

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

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

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

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

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

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

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

KP+05+SDA+NXX+ST gives the routing for an AT&T inward operator (see note 9).

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

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

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

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

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

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

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

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

ROUTING CODES

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

KP+1288+PIC+ST then KP+CC+cc+xxxxx+ST
KP+158+PIC+ST

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

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

(9) The format for an AT&T inward is usually KP+NPA+122+ST. In some small cities there is an extra code used called a Terminating Toll Center (TTC) or sometimes just a city code. If a TTC is used the format is KP+NPA+TTC+122+ST. To get an inward with most BOCs you dial KP+SDA+11591+ST but there are some which use a format of KP+SDA+TTC+121+ST. To get the inward routing for a particular exchange, use the Rate Quote System.

(10) The number for Rate and Route was 800+141+1212 but this was discontinued sometime last year, when the CBDS operators got a computer terminal called COMPIS. In each state there is an inward which acts like a Rate and Route operator. In New York it's 316+121.

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

(12) The marine operator is used in calling ships that are close to the United States. There is an operator called the "High Seas" operator who can be reached by dialing 800-SEA-CALL (800-732-2255). The High Seas operator is a service of AT&T, while Marisat is an independent company (see note 6). A High Seas call can go to any ocean for $4.50 for the first 3 minutes and $.99 for each additional minute. A Marisat only calls to 3 oceans and costs $10 dollars a minute.

(13) 1168 and 1168XX are used to verify an AT&T calling card number. For dial KP+NPA+1168XX+ST when you hear a "bong" you dial the calling card number. If you use 1168 you enter the number in touch tone and if you use 3282 you enter the card number in MF using KP and ST.

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

(continued on next page)

AT&T/BOC ROUTING CODES

(continued from previous page)

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

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

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

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

In July 87, we ran an article (How Phreaks are Caught) which included the 800 number allocation for long distance carriers. This is an updated list of the 800 exchanges that route directly to US Sprint: 800-326, 800-347, 800-359, 800-356, 800-546, 800-669, 800-726, 800-729, 800-733, 800-735, 800-736, 800-767, 800-776, 800-827, 800-877.

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

2600
PO BOX 99
Middle Island, NY 11953-0099

1986

[illegible]

1987 ISSUES ALSO AVAILABLE!

****

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

2600 BACK ISSUE ORDER:

☐ 1984 $25 ☐ 1985 $25 ☐ 1986 $25 ☐ 1987 $25

SEND THIS COUPON WITH PAYMENT TO:

2600 Back Issues
P.O. Box 752
Middle Island, NY 11953
(your address label should be on the back of this form)