2600

The Monthly Journal of the American Hacker

Volume 4, Number 12 December, 1987 $2

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Bobby Arwatt

Production
Mike DeVoursney

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

Cartoonists: Dan Holder, Mike Marshall.
Reader: John Kew.

Editor Emeritus TSH

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

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

Yearly subscription: U.S. and Canada - $15 individual, $40 corporate.
Overseas - $25 individual, $55 corporate.
Back issues available for 1984, 1985, 1986 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 (OSU NY): 914-725-4060
BBS #2 (CENTRAL OFFICE): 914-234-3260
USENET ADDRESS: 2600@dasys1.UUCP
ARPANET ADDRESS: phrl!dasys1!2600@nyu

Important News

A number of circumstances have forced us to make some changes in the way 2600 is published. As of 1988, we will become a quarterly publication instead of a monthly publication.

We've been printing 2600 under the "new" format for a year now. And one thing we can't help but notice is that it's frightfully expensive. We adopted this format so that we could present longer articles and also become a little more visible. And we have succeeded in both of these ambitions. However, if we were to continue at this pace, we would run out of funds entirely. The $15 we charge for an individual subscription is actually less than what it costs to produce one issue for a year. This is why we charge more to those that can afford more, namely corporations and large organizations where the magazine is passed around to many people. And this is why we continue to sell back issues. By providing alternate sources of income, we are able to continue to keep the magazine going at a low cost.

By raising the price to cover the costs of printing, mailing, and running an office, we could easily put the magazine out of the reach of most of our subscribers. We've seen publications smaller and less informative than ours with annual prices of over $100! We don't want to take that road.

By reducing the amount of times we publish during the year (at the same time increasing the size of each issue slightly), we can keep the price down, keep ourselves out of financial problems, and hopefully give ourselves more time to make each issue mean a little more.

This brings us to the time factor. We put a great deal of time into putting out the magazine. But 2600 is more than just a magazine. We're constantly trying to educate the populace on the uses and abuses of technology. We're told that as a result of our campaign to abolish the touch tone fee in New York, a bill may be introduced in the state legislature proposing just that. Our growing bulletin board network will do much to ensure freedom of speech for all computer users. And, of course, we want to make sure that people see and hear about this magazine and our organization, either by getting maximum exposure in the media or by getting international distribution. At our current frenzied pace, we just don't have the time to adequately pursue these goals. At a more relaxed pace, we feel we'll be better able to put out a quality publication and make it more memorable overall.

Naturally, we don't expect everyone to agree with our conclusions. If you feel strongly negative about this change or about anything else, we'll certainly give you a refund for the balance of your subscription. We hope, though, that you'll stick it out at least to the first issue of our quarterly format to see if we live up to your expectations.

Our spring issue will be mailed on or around March 15, 1988. Subsequent mailing dates are scheduled for June 15, September 15, and December 15. Your expiration date will be adjusted in the following manner: January, February, and March will end with the spring issue; April, May, and June—summer; July, August, and September—fall; and October, November, and December—winter.

A number of subscribers have complained about their issues arriving late or sometimes not at all. It appears we must become militant in convincing the post office to do their job. If you do not get an issue within a week of when we send it out, you should call us and call your post office. Usually it is the post office on the receiving end that is at fault.

As always, we welcome your feedback on what we're doing. We hope this change results in a better publication and a stronger Twenty Six Hundred.

HACKING IBM'S

by Lex Luthor
and The Legion of Hackers

Command Interpretation Chart: The following chart shows some VM/CMS commands with their equivalent UNIX and VAX/VMS commands. This will allow those readers who are familiar with other operating systems to quickly reference the CMS counterparts.

VAX/VMS	UNIX	VM/CMS	explanation
/NOCOMMAND	*NONE*	NOIPL	aborts login pgm
SHOW USERS	who	QUERY NAMES	online userlisting
DIRECTORY	ls	LISTFILE	
		or FILELIST	show current dir.
TYPE filename	cat filename	TYPE fname	
		ftype fm	list or view files
EDIT	ed or vi or ex	XEDIT	system editor
DELETE file	remove filename	ERASE fname	
		ftype fm	deletes files
PHONE user	write user	TELL userid	user communication
Control Y	Ctrl-Backslash	Hard-break	
		then HX	aborts process

Corresponding files:

SYSUAF.DAT	/ETC/PASSWO	USER DIRECT	Userlist & user information
MAIL.TXT	USR/MAIL/ user	USERID NOTE	Electronic mail files
LOGIN.COM	.PROFILE	PROFILE EXEC	User login command files

Local Commands:

Local commands are written for an individual system, and customized to suit a facility's needs. (These commands are execs which are either not available from IBM or are cheaper to write on your own.) I will mention a few which may be found on other systems, as these are rather common.

WHOIS

This command gives a little information about any user that you specify who is on the system. This is similar to the UNIX command "finger".

.WHOIS MAINT BACKUP MAILER BUBBA RELAY VMUTIL

Userid	Name
MAINT	System Maintenance Account
BACKUP	VM System Backup and Recovery Machine
MAILER	BITNET Inter Node Mail Processing Machine
BUBBA	Bubba B. Bonehead—Programmer/analyst Extroadinaire
RELAY	BITNET Internet Chat Facility
VMUTIL	VM Utilization Statistics

SYSPASS
READPW
WRITEPW

In most cases, the only way to change a user's password is by having the system operator or someone with high privileges do it. This is one reason why many passwords remain the same for long periods of time. These programs allow users to change their logon password (SYSPASS), read access minidisk password (READPW), and write access minidisk password (WRITEPW). You may find these or similar programs on some systems.

Privileged Commands

As far as I know, there is no command to determine which privilege class the userid you are using is. The only way to find out is to check in the CP Directory. The following are some privileged commands and what privilege class is needed to run them. From what I've seen, the system keeps no records of failed attempts at running privileged commands. Successful uses of these commands are most likely recorded, either in a log or by sending a message to the system console or both, especially when using FORCE.

FORCE userid (Class A)

This command will forcibly log off the userid you specify. I really can see no reason other than to be a total idiot for abusing this command.

DISABLE raddr (or) all (Class A or B)

This is used to prevent specific terminals or all terminals from logging onto the system. Again, there is no real reason to use this or most other privileged commands unless you want to be kicked off of the machine. If you do DISABLE a terminal, simply use ENABLE to repair the damage.

DETACH realaddr (FROM) whatever (Class B)

This is used to detach real devices from the system. These can be terminals, printers, disk packs, tape drives, etc. You must know the real address of the device, and "whatever" can be the system name, or a userid.

WARNING userid (or) operator or all (Class A or B)

VM/CMS—PART TWO

Warning will send a priority message to a user, operator, or all users on the system. It will interrupt anything they happen to be doing. Obviously sending a msg to all users stating they are BONEHEADS is not recommended.

Minidisks

A minidisk is a subdivision of consecutive cylinders on a real DASD volume. The real DASD device is the actual disk the information is stored on. This can be compared to a hard drive for an IBM PC. Before the drive can be used, it must be formatted. Once formatted, it is divided up into directories called minidisks. Minidisks are measured in cylinders, which are the standard memory storage units. There can be many minidisks on a DASD. Associated with each CMS disk, is a file directory, which contains an entry for every CMS file on the disk. A minidisk can be defined for R/W or R/O (read/write or read/only) access. It can also be used for storage of files. Each minidisk has a virtual address which can be from 001-5FF (hexadecimal) in basic control mode, and 001-FFF in ECMODE (Extended Control Mode).

CMS minidisks are commonly accessed by a letter of the alphabet (A-Z). For example, let's assume we are logged onto a VM/CMS system under the userid of JOE. We want to see what minidisks we have access to. We use the QUERY SEARCH command to determine which disks we are ATTACHed to.

```
.Q SEARCH

JOE001      191     A       R/W
JOE002      192     D       R/O
CMS190      190     S       R/O
CMS19E      19E     Y/S     R/O
```

Each minidisk has a volume name, virtual address, filemode, and access mode. The A disk is the default. Most accounts you gain access with will have an A disk with a virtual address of 191. The S disk is the System disk. This contains the files and programs for running the system. The same goes for the Y disk. The D disk is another disk used by JOE.

You can view what each of these directories contains by issuing the LISTFILE command.

```
.LISTF

BUBBA       NOTE        A1
MISC        WHATEVER    A1
PROFILE     EXEC        A0
```

This is a list of files on the A disk. The first column is the filename, the second is the filetype, and the third is the filemode. Filenames can be anything you specify. Filetypes can also be anything you specify, but commonly follow a pattern which tells what type of file it is. Filemodes are comprised of a filemode letter (A-Z) and a filemode number (0-6).

Filenames can contain the following characters: A-Z, 0-9, $, #, +, -, :.

Here is an explanation of common filetypes:

Filetype Description

DATA Data for programs or simply TYPE-able text.

EXEC User written programs or IBM procedures written in REXX.

HELP System HELP files.

HELPCMS System HELP files.

LANGUAGE One of the languages that the system supports, such as ASSEMBLE, COBOL, FORTRAN, JCL, REXX, PL1, SNOBALL, BINARY, etc.

LISTING Program source code listings

LOADLIB Loading Library

MACLIB Macro Library

MODULE System commands

NETLOG Contains a list of all files which have been SENT to other users.

NOTE Similar to E-MAIL on other systems, a note sent from another user.

SOURCE SOURCE code for various programs.

TEXT Text file. Probably used for programs and when TYPEd yields little.

TXTLIB Text Library

WHATEVER A nonstandard filetype which will probably be somewhat descriptive of its contents.

XEDIT A file which was created using the XEDIT utility.

Both filenames and filetypes must not exceed eight characters in length.

Filemodes

Filemode numbers are classified as follows:

Filemode 0: There is little file security on VM/CMS. This may be due to the fact that directory security is very good. A file with a mode

(continued on next page)

HACKING IBM'S

(continued from previous page)

of zero makes that file invisible to other users unless they have Read/Write access to that disk. When you LINK to someone's disk in Read/Only mode and get a directory listing, files with a mode of 0 will not be listed.

Filemode 1: This is the default filemode. When reading or writing files, you do not have to specify this filemode number (unless you want to) since it will default to it.

Filemode 2: This is basically the same as a filemode of 1. It is mainly assigned to files which are shared by users who link to a common disk, like the system disk.

Filemode 3: Be careful when you see these! These are automatically erased after they have been read. If a file with a mode of 3 is printed or read it will be erased. Blindly reading files without paying attention to the filemode numbers can shorten your stay on a system. The main reason for this filemode is so the files or programs that are unimportant or have one-time use can be automatically deleted to keep disk space and maintenance to a minimum.

Filemode 4: This is used for files that simulate OS data sets. They are created by OS macros in programs running in CMS. I have not found any files with this filemode, so for the time being, you should not be concerned with it.

Filemode 5: This is basically the same as filemode 1. It is different in that it's used for groups of files or programs. It makes it easier for deleting a number of files that a user wants to keep for a certain period of time. You could just enter: ERASE * * A5. Now all files on the A disk with a filemode of 5 will be deleted.

Filemode 6: Files with this mode are re-written back to disk in the same place which is called "update-in-place". I have no idea why this would be specified, and have not found any files with a filemode of 6.

Filemode 7-9: These are reserved for IBM use.

Accessing Information

Looking back at our Q SEARCH listing, let's see what is on the D disk:

```
.LISTF * * D

NOTMUCH ONHERE D1
```

In this case, the D disk only contains one file called NOTMUCH with a filetype of ONHERE. But do not forget the fact that you only have Read/Only access to the D minidisk! So there may or may not be merely one file on the D disk. Remember all filemodes of 0 (which in this case would be D0) are invisible to anyone who does not possess Read/Write access.

You can access any disk that you are ATTACHed to by replacing the D in the above example with the filemode letter (A-Z) you want to access. As was shown previously, the QUERY SEARCH command will give you a list of minidisks that your userid is attached to upon logging in. These command statements are usually found in your PROFILE EXEC.

So you can access a few minidisks. There may be hundreds on the system. Unlike UNIX and VMS, and most other operating systems for that matter, you cannot issue a command and some wildcard characters to view the contents of every user's directory. In order to access another users' directory (minidisk) you must have the following: 1) The USERID of the person whose disk you wish to access; 2) The virtual address(es) (CUU) that the USERID owns; 3) The Read, Write, or Multi disk access password, depending on which access mode you wish to use.

This would be accomplished by the following:

```
.LINK TO BUBBA 191 AS 555 RR

Enter READ link password:
 **************************
 HHHHHHHHHHHHHHHHHHHHHHHHHH
 SSSSSSSSSSSSSSSSSSSSSSSSS
.RBUBBA

R; T=0.01/0.01 21:58:48
.ACCESS 555 B

R; T=0.01/0.01 21:59:03
.Q SEARCH

JOE001    191    A    R/W
BUB001    555    B    R/O
JOE002    192    D    R/O
CMS190    190    S    R/O
CMS19E    19E    Y/S  R/O
```

VM/CMS—PART TWO

.LISTF * * B

MISCFILE	**OATA**	**B1**
PROFILE	**EXEC**	**B1**

.REL 555

R; T=0.01/0.01 22:02:01

Now an explanation of the events which have just occurred.

The LINK command is used to access other users' minidisks. The format is:

.LINK (TO) USERIO VADDR1 (AS) VADDR2 (MODE) ((PASS=)PASSWORD)

BUBBA is the USERID whose disk we wish to access. VADDR1 is a virtual address which belongs to the BUBBA userid. If BUBBA was to access our minidisk whose userid is JOE, he could access either our 191 address or our 192 address. The 190 and 19E addresses are usually automatically accessed by nearly all the users of the system since it contains system commands. We are assuming that BUBBA indeed has a minidisk with the virtual address of 191. Some userid's may not have any or they may have addresses which are somewhat obscure, say of 13A or 503. The only way we would be able to access those assuming BUBBA did not give them to us would be to guess them. This would be rather difficult, time-consuming, and dangerous as we will soon see.

VADDR2 is any address which is not currently in our control (i.e., in our Q Search which would be 190, 191, 192, 19E) and is in the range of 001 to 5FF in Basic Control or FFF in Extended Control. In this example, we chose to use 555. We could have easily used 104, 33F, 5FA, etc.

MODE is the access mode which consists of up to 2 letters. The first letter specifies the primary access mode. The second letter is optional and designates the alternate access mode. If the primary mode is not available, the alternate is used.

The access mode we used was RR. Valid access modes are:

R: Primary Read/Only access. This is the default. You can opt to not specify an access mode when linking to a user's disk, and this is the mode which is used. It will only work if no other links are in effect.

RR: This allows read access no matter what links are in effect to that user's disk.

W: Primary Write access. This is only good if no other links are in effect.

WR: If Write is available then the link will be made. If not it will go to Read.

M: Primary Multiple access.

MR: Resorts to Read if Multi is unavailable.

MW: This guarantees write access no matter what.

If another user has write access to one of your disks when you log on, your access will be forced to Read/Only. For this reason, you should have read access to other disks instead of write. If you wish to see what files have a filemode of zero, then link with write access, view, or access those files, then RELEASE the disk and re-access it via read to avoid suspicion by that user of unauthorized individuals gaining write access to his files.

If a user has write access to a disk, you cannot gain write access unless you use a mode of MW. It is not recommended to have write access to another's disk if they themselves have write access. CMS cannot guarantee the integrity of the data on a disk which has more than one person linked to it with write access. Now if you see that the user is in a disconnected (DSC) state through the Q NAMES command, then it shouldn't be a problem if you also have write access since the person is not active. If that person reconnects, however, then it is advisable to RELEASE that disk as soon as possible to avoid any chance of data being destroyed.

PASS=PASSWORD. Like the logon password, it can be a 1-8 character string that *must* match the access mode password for the VADDR1 of the userid which you are attempting to gain access to. Up to three access mode passwords can exist for each minidisk—R, W, and M.

If the installation uses the Password Suppression Facility, an INVALID FORMAT message will be issued when you attempt to enter the password for a disk on the same line that the LINK command was entered on. Obviously this is to prevent people from "spoofing" the password off the screen or from printouts found in the trash. If this occurs, just hit

(continued on page 14)

the telecom informer

If you've suddenly forgotten how to use custom calling features, the folks at Southwestern Bell have a handy service for you. It's a special interactive number that gives you information on how to use certain features ("press 1 for call waiting info, 2 for call forwarding, etc."). The number is 713-621-2949. Keep in mind, though, that instructions for using custom calling features vary from company to company....We probably all heard something about the "Max Headroom" incident in Chicago – a video pirate somehow overpowered the signals of two local stations on different nights, dressed in Max Headroom gear and making obscene gestures. We've heard all kinds of theories as to how it was done. Most of these seem to agree that it's ridiculously easy to overpower a local station on their microwave links the real trick is finding their path. Unlike the Captain Midnight spectacle, not many people believe this bandit will ever be caught because apparently there is no real way of tracing such an action, other than having eyewitnesses. We hope to be able to get more specific information. It looks like some fun lies ahead. ...AT&T and Indiana Bell have linked forces to combat long distance fraud. Their new service, called the Revenue Protection System (doesn't that sound like a mobster term?) allows interexchange carriers to share information on network misuse and credit histories. Carriers will be able to obtain data on calls to and from particular numbers to trace fraud more easily. Participating long distance companies must feed their credit information into the database every month. Depending on their own networks, these companies could then access the system by using analog lines, digital, or private line links, such as the Ameritech Packet Switched Network. The folks at the national Communications Fraud Control Association of Fairfax, Virginia have endorsed this new service....Police hope a teenage computer "whizkid" arrested for theft and intercepting computer data in Burlington, Canada will help them bust a hacker network that spans the entire province of Ontario. The investigation started in October when Westinghouse Canada complained to Hamilton police that an outsider had broken into their Private Branch Exchange (PBX) and billed more than $1,000 in long-distance computer calls to the company. A Westinghouse spokesman said the youth was "unselfish", passing the entry code among computer hackers around the world. "He was using our computer system to use other computers and bulletin boards," he said. The final telephone tab could reach $10,000 but Westinghouse hasn't decided if it will seek restitution in the courts. Police said the youth was using a basic computer, a Commodore 64, to break through sophisticated security systems. The teen's records showed five other computer systems – three belonging to multi-national corporations in Southern Ontario – were entered but criminal charges weren't laid because the companies weren't aware of the intrusions....ITT has announced that its long distance unit, U.S. Transmission Systems Inc. (USTS), will drop the surcharge for "950" calls placed by customers with ITT calling cards. Virtually all long distance carriers charge subscribers a fee to access "950" services. Previously, ITT card customers paid a 50-cent surcharge for each call placed over the ITT network....BellSouth will be the first Regional Bell Operating Company to try out what promises to be a significant new service known as the Intelligent Network. This network will be able to handle a variety of tasks by interacting with a group of Bellcore-developed specialized databases. According to *CO*

Magazine, the Intelligent Network will improve Bell Operating Company (BOC) equipment efficiencies in the handing off of 800 customers to interexchange carriers, enhance interexchange competition, and enable customers to easily change their interexchange carriers without changing their 800 numbers. What this means is that customers won't have to change their 800 numbers if they decide to switch long distance companies. Call handling will not be limited to switches. Calls will be handled by the remotely located database and distributed throughout the network....British Telecom is marketing as part of its "advanced business systems" a product known as QWERTYphone. It's a desk-top terminal with alphanumeric, function and telephone number keys plus four-line LCD. It's being demonstrated as a low-cost computer and speech terminal. They also are promoting LEKTOR, a high-security data encryption unit that protects data against eavesdroppers, provides user authentication, and offers a simplified key management system. And of course, there's Skyphone, enabling travelers to keep in touch while they're in the sky with the rest of us down here on the ground. All paid for by credit card, of course. Popular features on new British Telecom phones: ten number memory, secrecy button, last-number redial and dual signaling, plus one-button access to network and PBX facilities....Israel is creating a computerized database with a wide range of personal information about Arab residents of the West Bank and Gaza Strip. According to a report by the West Bank Data Base Project, a widely respected Israeli research institute monitoring developments in the occupied territories, the new Israeli Ministry of Defense database amounts to a "computerized carrot-and-stick operation" and a potential "big brother" for the West Bank and Gaza Strip. The computer, which began operating over the summer, is being programmed with information on property, real estate, family ties, political attitudes, involvement in illegal activities, licensing, consumption patterns, and occupations of Arab residents of the West Bank and Gaza. It is particularly dangerous, the report says, because the normal Israeli laws and checks and balances governing the use of databases do not apply to the occupied territories. By pressing a key on a computer terminal, any Israeli official working in the occupied territories will be able to gain access to lists of names of those Arabs who are "positive" and those who are "hostile". This information could be used to decide the fate of their applications for anything from car licenses to travel documents.

all about BLV

Verification and emergency interrupts are two operator functions that have always fascinated the phone phreak world. Here then is an explanation of just how it all really works. (Note: this article is written solely on the AT&T TSPS process of verification.)

Let's say Smith needs to get ahold of his friend, Jones. Jones' telephone line is busy, and Smith must talk to Jones immediately. He calls the operator, by dialing 00 for an AT&T TSPS Operator (or in some areas, 0 still gets TSPS). The operator answers, and asks if she can help him. Smith replies that he needs to interrupt a call in progress so he can get through. He tells the operator Jones' number. After a few seconds, he is connected to Jones and they talk.

The name for this process is Busy Line Verification, or BLV. BLV is the telco term for this process, but it has been called "Verification", "Autoverify", "Emergency Interrupt", "Break into a line", "REMOB", and others. BLV is the result of a TSPS that uses a Stored Program Control System (SPCS) called the Generic 9 program. Before the rise of TSPS in 1969, cordboard operators did the verification process. The introduction of BLV via TSPS brought about more operator security features. The Generic 9 SPCS and hardware was first installed in Tucson, Daytona, and Columbus, Ohio in 1979. By now virtually every TSPS has the Generic 9 program.

A TSPS operator does the actual verification. If Jones was in the 314 Area code and Smith was in the 815 Area code, Smith would dial 00 to reach a TSPS that served him. Now, Smith, the customer, would tell the operator he needed an emergency interrupt on a given number, 314+555+1212. The 815 TSPS operator who answered Smith's call cannot do the interrupt outside of her own area code, (her service area), so she would call an Inward Operator for Jones' area code, 314, with KP+314+TTC+121+ST, where TTC is an optional Terminating Toll Center code that is necessary in some areas. Now a TSPS operator in the 314 area code would receive the 815 TSPS operator's call, but a lamp on the 314 operator's console would tell her she was being reached with an Inward routing. The 815 operator then would say something along the lines of she needed an interrupt on 314+555+1212, and her customer's name was J. Smith. The 314 Inward (which is really a TSPS) would then dial Jones' number, in a normal Direct Distance Dialing (DDD) fashion. (DDD by an operator is really called ODDD, for Operator Direct Distance Dialing.) If the line was not busy, then the 314 Inward would report this to the 815 TSPS, who would then report to the customer (Smith) that 314+555+1212 was not busy and he could call as normal. However, if the given number (in this case, 314+555+1212) was busy, then the process of an Emergency Interrupt would begin.

The 314 Inward would seize a verification trunk (or BLV trunk) to the toll office that served the local loop of the requested number (555+1212). A feature of the TSPS checks the line asked to be verified against a list of lines that should not be verified, such as radio station call-in lines, police station lines, etc. If the line number a customer gives is on this software list, then the verification cannot be done, and the operator notifies the customer. The 314 Inward would then press her VFY (VeriFY) key on her TSPS console, and the equipment would outpulse (onto the BLV trunk) KP+0XX+NXX+XXXX+ST. The KP signal prepares the trunk to accept MF tones, the 0XX is a "screening code" to protect against trunk mismatching, the NXX is the exchange or prefix of the requested number (555), the XXXX is the last four digits of the requested number (1212), and the ST is the STart signal which tells the verification trunk that no more MF digits follow. The screening code is there to keep a normal Toll Network (used in regular calls) trunk from accidentally connecting to a verification trunk. If this screening code wasn't present, and a trunk mismatch did occur, someone calling a friend in the same area code might just happen to be connected to his friend's line, and find himself in the middle of a conversation. But the verification trunk is waiting for an 0XX sequence, and a normal call on a Toll Network trunk does not outpulse an 0XX first. (Example: You live at 914+555+1000 and wish to call 914+666+0000. The routing for your call would be KP+666+0000+ST. The BLV trunk cannot accept a 666 in place of the proper 0XX routing,

busy line verification

and thus would give the caller a re-order tone.) Also, note that the outpulsing sequence onto a BLV trunk cannot contain an area code. This is the reason why if a customer requests an interrupt outside of his own NPA, the TSPS operator must call an Inward for the area code that can outpulse onto the proper trunk. If a TSPS in 815 tried to do an interrupt on a trunk in 314, it would not work. This proves that there is a BLV network for each NPA, and if you somehow gained access to a BLV trunk, you could only use it for interrupts within the NPA that the trunk was located in.

BLV trunks "hunt" to find the correct trunks to the right Class 5 end office that serves the given local loop. The same outpulsing sequence is passed along BLV trunks until the trunk serving the toll office that serves the given end office is found.

There is usually one BLV trunk per 10,000 lines (exchange). So, if a toll office served ten central offices, that toll office would have ten BLV trunks running from a TSPS site to that toll office.

Scrambling the Audio

The operator (in using the VFY key) can hear what is going on on the line (modem, voice, or a dial tone, indicating a phone off-hook), but in a scrambled state. A speech scrambler circuit within the operator console generates a scramble on the line while the operator is doing a VFY. The scramble is there to keep operators from listening in on people, but it is not enough to keep an operator from being able to tell if a conversation, modem signal, or a dial tone is present upon the line. If the operator hears a dial tone, she can only report back to the customer that either the phone is off-hook, or there is a problem with the line, and she can't do anything about it. This speech scrambling feature is located in the TSPS console, and *not* on verification trunks. In the case of Jones and Smith, the 314 Inward would tell the 815 TSPS, and the 815 TSPS would tell the customer. If there is a conversation on line, the operator presses a key marked EMER INT (EMERgency INTerrupt) on her console. This causes the operator to be added into a three way port on the busy line. The EMER INT key also deactivates the speech scrambling circuit and activates an alerting tone that can be heard by the called customer every 10 seconds. This tone tells the customer that an operator is on the line. Some areas don't have the alerting tone, however. Now, the operator would say "Is this NXX-XXXX?" where NXX-XXXX would be the prefix and suffix of the number that the original customer requesting the interrupt gave the original TSPS. The customer would confirm the operator had the correct line. Then the operator would say, "You have a call waiting from (customer name). Will you accept?" This gives the customer the chance to say "yes" and let the calling party be connected to him, while the previous party would be disconnected. If the called customer says "no", then the operator tells the person who requested the interrupt that the called customer would not accept. The operator can just inform the busy party that someone needed to contact him or her, and have him/her hang up, and then notify the requesting customer that the line is free. Or, the operator can connect the calling party and the interrupted party without loss of connection.

If a customer requested an interrupt upon a line within his home NPA (HNPA), then the original answering TSPS operator would do the entire verification process as described above.

The charges for this service (in my area at least) run $1.00 for asking the operator to interrupt a phone call so you can get through. There is an 80 cent charge if you ask the operator to verify whether the phone you're trying to reach is busy because of a service problem or because of a conversation. If the line has no conversation on it, there will be no charge for the verification.

The Aftermath

When the customer who initiated the emergency interrupt gets his telephone bill, the charges for the interrupt call will look similar to this:

```
12-1   530P   INTERRUPT CL
       314 555 1212   OD   1   1.00
```

The 12-1 is December First of the current year, 530P is the time the call was made to the operator requesting an interrupt. INTERRUPT CL is what took place, that is, an interrupt call. 314 555 1212 is the number requested. OD stands for Operator assisted. Daytime call, the 1 is the

(continued on page 12)

Switch-Hook Dialing

Dear *2600*:

After recently reading some old textfiles on switch-hook dialing, I've been trying to practice my speed. Switch-hook dialing comes in handy when you just happen to be at a phone that has a dial lock or some other device restricting dialing. I can now switch hook dial on almost any phone but when I try to do it on a payphone, it hardly ever works properly. Why is this?

JS
Dallas, TX

The switch hook in a Western Electric AT&T payphone has a mercury switch in it. The way this works is when the hook switch is at an angle a small ball of mercury rolls down onto two contacts. If you were to rapidly depress the switch hook on a payphone, it would take time for the ball of mercury to roll back and forth thus disturbing the timing of your dialing. The time it takes for the mercury to make or break contact can be long enough to appear that you are dialing a new digit. Why do pay phones have these mercury switches in the first place? We assume it's because they tend to be more durable. By the way, the best way to defeat a dial lock is to simply carry a touch tone pad (also known as a "white box").

Pen Registers

Dear *2600*:

I was wondering if it would be possible for you to have a listing of all the 2600 support BBS's around the country? I for one would be extremely interested, and I'm sure there are many others out there like me.

Also, my school has a "regulation" pen register on all their lines. I am currently trying to gain any information from it that I can. But for now, I need to know if there is any way of determining if you *have* a pen register on your line. Strange things have been happening on my line, and I was wondering if there is any sure way of telling if your line is being monitored or tapped by good old Ma Bell. Any help or suggestions would be appreciated.

Norman Bates

First off, we have two bulletin boards online at 914-725-4060 and 914-234-3260 and quite a few others that have expressed interest in becoming 2600 bulletin boards. We will announce their numbers when the time comes.

Some people claim they can tell when there's a pen register on their line by hearing strange clicks or tones. In some cases this may very well be true but certainly not in all. For example, someone could plug in a Radio Shack pen register anywhere on your line and it would not make any strange noises over the phone. The phone company itself is one of the easier culprits to track down. If they have a pen register on your line, you can often find out by befriending someone in the switchroom. It's a simple matter of asking any acquaintances you have there whether or not there is something strange attached to your line. When the phone company does it legally, they're often required to tell you at some point. The harder culprits are those that are doing it outside the law where the possibilities are almost endless. As microwave and satellite hacking becomes more commonplace, it's likely that passive eavesdropping will increase. Since no direct contact with a particular line is necessary, this method is completely untraceable. And naturally, you won't hear any telltale clicks on your line.

Evil Happenings

Dear *2600*:

There really is a big "brother". They are the C.F.R. and the Trilateral

LETTERS

Commission. Their goal: a one world government and a one world money system. Computers will play a key role. This is why the crackdown on hacking and billboards is on.

Paia Jones

Thanks for this interesting bit of news.

Canadian Questions

Dear *2600*:

I think you have a great mag. Is there a store that I can go to every month to buy your mag in Canada? Do you know a Canadian address where I can get hacking software for the Commodore 64 or an IBM clone? I would like both, most likely communication and deprotection utilities.

PG
Toronto

We don't have any distributor in Canada so you won't find us in any stores. As far as software, since we really don't handle that kind of thing we suggest putting a free ad in the 2600 Marketplace or asking around on bulletin boards.

Speaking of stores, here are the ones you can find us in in New York City: Apostrophes Books, 660 Amsterdam Avenue; Coliseum Books, 1771 Broadway; Soho Zat, 307 West Broadway; Hudson News—Kiosk, 753 Broadway; Spring Street Books, 169 Spring Street; Papyrus Books, 2915 Broadway; St. Mark's Bookshop, 13 St. Mark Street; Shakespeare Books, 2259 Broadway; B. Dalton's Booksellers, 396 6th Avenue; and College Stationery, 2951 Broadway.

The Truth Revealed

Dear *2600*:

What's the difference between Box 99 and Box 752?

Cheshire Catalyst

Besides being on separate ends of the post office with 652 other boxes between them, there is a very fundamental difference: Box 752 is for subscription information and Box 99 is for editorial submissions and letters. You played it safe by sending your letter to both boxes. This is a reply to the letter sent to the proper box, namely Box 99. The other letter was sent to the wrong box and, as a result, was ripped to shreds and burned.

Ingenious Solution

Dear *2600*:

I may have found the solution to the problem of not being able to store issues of 2600 since you went to the "booklet" format. If you take a plastic diskette holder such as the ones pre-punched to fit into the small 3-ring notebooks, you will see that 2600 is just a little too big to fit inside the pocket designed for the diskette. However, take a blow dryer and heat the plastic insert. When it is fairly warm, grab each side and stretch the insert! Now, 2600 will fit neatly inside the pocket and can be put in the 3-ring notebook. A whole year will fit nicely in 6 plastic inserts and now the notebook can be placed in your bookshelf along with your other classic books! These

(continued on page 16)

HACKING IBM'S

(continued from page 7)

return after entering the access mode, and wait for the enter password response.

Every disk password along with every user's password and other information is contained in the CP Directory. If the password is "ALL" then a password is not required for any user so you will not be asked for one. You will then receive a ready message indicating that the transaction has just been completed.

If you receive the message: "BUBBA 191 NOT LINKED; NO READ PASSWORD", then within the CP Directory, there is no read password at all. This means that the only way you can gain access to BUBBA's directory would be by getting his logon password. One note—I believe that a user's logon password cannot be any of his access mode passwords. The reasons for this are obvious. If BUBBA wants JOE to access a disk, then he can give JOE the corresponding disk password. If this was identical to his logon password then JOE could logon as BUBBA and access all of BUBBA's disks with no problem, and at the same time possess all of the privs that BUBBA has. Within the CP directory, if there is no password entry for read access then there are no entries for write or multi. If there is no entry for write then there may or may not be an entry for read, but definitely not one for multi. And finally, if there is no entry for multi then there may or may not be entries for read and write.

The methods for obtaining disk access passwords are the same as anything else. Common sense and "Password Psychology" come into account along with the element of luck.

Assume the userid is VMTEST and you are hacking the READ password. Passwords may be: RVMTEST, RVM, RTEST, RTESTVM. Others may be READ, READVM, VMREAD, READTEST, TESTREAD, and even VMTEST. Of course it could be something like: J2*Z5. Many times the same password will be used for R, W, and M access instead of three separate passwords.

CP keeps track of unsuccessful LINK attempts due to invalid passwords. When you exceed the maximum number of incorrect password attempts, which usually defaults to 10, the link command will be disabled for the remainder of your stay on the system. All you have to do is re-logon and you will have full use of LINK again.

If the LOGON/AUTOLOG/LINK journaling facility is activated, unsuccessful link attempts due to the above are recorded. When the threshold is reached the userid whose password you are trying to hack is sent a message. Therefore, keep track of the number of attempts you make and keep just short of the system threshold.

After successfully linking to a user's disk, you must issue the ACCESS command in order to get a directory listing or access any files on that disk. This is accomplished by:

.ACCESS VADDR2 B

VADDR2 is the address after "AS" in your link command line, and "B" is the filemode letter which you wish to access the disk as. This can be anything but the letters which you have already assigned up to a total of 26 (A-Z).

After accessing the disk to your heart's content, you can then RELEASE it. When you logoff, the disk is automatically released. Releasing the disk is not necessary unless you already are attached to 26 minidisks, and you want to access more. You would then release whatever disks you wish and link to access others. After releasing a disk, to re-access it you do not have to issue another link command but merely the ACCess command and what filemode you wish it to be.

The QUERY DASD command will list the minidisks that most everyone on the system has access to. All of these may or may not be automatically accessed upon logon. For this reason, you should issue it. Then all you have to do is ACCess the virtual address and define the filemode.

.Q DASD

DASD	**190**	**3380**	**SYSRES**	**R/O**	**32 CYL**
DASD	**191**	**3380**	**SYSRES**	**R/W**	**1 CYL**
DASD	**192**	**3380**	**SYSRES**	**R/O**	**2 CYL**
DASD	**193**	**3380**	**SYSRES**	**R/O**	**19 CYL**
DASD	**194**	**3380**	**SYSRES**	**R/O**	**21 CYL**
DASD	**19E**	**3380**	**SYSRES**	**R/O**	**27 CYL**

VM/CMS—PART TWO

In our Q SEARCH list, we have access to 190 as the system disk, 191 as our A disk, 192 as our D disk, 19E as the system's Y disk. Both 193 and 194 are accessible but have not been accessed by us. Thus:

```
.ACC 193 B
B (193) R/O
.
```

Now the 193 disk is our B disk and accessible by us. We can perform the same procedure for the 194 disk.

DIRMAINT

The Directory Maintenance utility can be found on some systems. If it is running, DIRMAINT should be a valid userid. The DIRMAINT userid is automatically initialized when the system is started up. It remains in "disconnected" mode awaiting transactions which contain directory maintenance commands.

If you come across a system with DIRMAINT, it will provide you with all the information you need to know about it. A few commands are important, at least to the hacker:

MDPW: This displays access passwords for one or all of that userid's minidisks.

```
.DIRM MDPW
DVHDIR005R ENTER CURRENT CP PASSWORD TO
VALIDATE COMMAND OR A NULL TO EXIT:
R; T=0.12/0.15 19:33:34
 DVHMDF3011 MINIDISK 191:          RBUBBA
                        WBUBBA    MBUBBA
 DVHMDF3011 MINIDISK 192:          RBUBPW
                        BONEHEAD  MULTIBUB
```

The reason you must enter the user's logon password is obvious. If someone walks up to a user's terminal and wants to know what the guy's disk passwords are all he would have to do is enter this command and he would get them, except for the fact that it does ask for the user's logon password, thus protecting the disk passwords.

Help: Get more info on DIRM commands.

PW: This changes a user's logon password.

PW?: Find out how long it was since the user changed his logon password.

MDISK: Change access mode, change, add, or delete passwords.

LINK: Cause an automatic link, at logon, to another user's minidisk.

FOR: Enter a DIRMaint command for another user if authorized.

Things You Want

Things you want are: more valid userid's to try passwords on, actual logon passwords, and disk access passwords. Obtaining userid's can be accomplished by using the Q NAMES command every time you logon. Obtaining logon passwords isn't as simple. There are a couple of places that you will want to explore.

The AUTOLOG1 or AUTOOP virtual machines (userid's) usually auto-logon other userid's. Now, in order to do this they must have those users' passwords. These are contained within various EXECs within their user directory. If you can obtain a valid disk access password for whichever one of these is running on your particular system, you can get more passwords and possibly some disk access passwords for about 10 other userid's. This should allow you to get more disk access passwords and hopefully more logon passwords. Nevertheless, having obtained a few more passwords, and not using them until the original one you hacked dies, will greatly extend your stay on the system.

EXEC files from any user may contain more disk access passwords for other users and those users' directories may contain EXECs which have more passwords, and so on. Of course many other types of files may contain this type of infonmation.

The CP directory—this is similar to a big bullseye on a target. This directory, as previously explained, contains users' passwords, various system information, and minidisk passwords. The directory usually goes under the filename/filetype of USER DIRECT. It can be anywhere on the system, and can have a different name, which in my view would add to system security. It is usually found in either or both of two users' directories which I leave to you to find (sorry). This is a very big weakness in CMS due to the fact that if you can find what userid the directory is in, and its disk access password, you've got the system by the balls. The file may

(continued on next page)

HACKING VM/CMS

(continued from previous page)

also have a filetype of INDEX which is a compilation or sorting of pertinent information used for speeding up various procedures the system carries out constantly. A typical entry in the USER DIRECT file would look like:

```
USER BUBBA BUBAPASS 1M 3M BG

VMU01000
 ACCOUNT 101 SYSPROG

VMU01010
 IPL CMS

VMU01020
 CONSOLE 00D 3215

VMU01030
 SPOOL 00C 2540 READER *

VMU01040
 SPOOL 00D 2540 PUNCH *

VMU01050
 SPOOL 00E 1403 A

VMU01060
 LINK MAINT 190 190 RR

VMU01070
 LINK MAINT 190 19D RR

VMU01080
 LINK MAINT 19E 19E RR

VMU01090
 MDISK 191 3350 152 003 VMPK01 MR RBUBBA
                          WBUBBA MBUBBA
 MDISK 192 3350 152 003 VMPK01 MR RBUBPW
                          BONEHEAD MULTIBUB

VMU01100
*
```

The first line gives the userid of BUBBA, password BUBAPASS, 1 and 3 Megs of virtual memory, and Privilege Classes B and G. The next line gives the account number and department or owner of the account. The next few lines define miscellaneous system information. Next, three lines of what disks should be automatically linked to upon logon. And finally the minidisk (MDISK) virtual addresses and corresponding passwords.

Conclusion

As usual, there is always more I could add to an article like this one. I did not want to keep writing part after part so I wrote a "complete" article on Hacking VM/CMS. I apologize for the length but I wanted to mention everything you needed to become familiar with the operating system and its security/insecurity. I intentionally "forgot" to mention various bits of information which would put sensitive and destructive information in the hands of anyone who reads this article. The information within this article can and will be different from system to system so don't take anything too literally. This article is comprised of 80% information from actual system use, 10% CMS help files, and 10% from various CMS documentation. I may write a followup article of shorter length as more people become familiar with CMS.

DECEMBER'S LETTERS

(continued from page 13)

inserts can be purchased at many office supply stores, discount centers, and department stores. I am enclosing a sample insert for you to try out. Heat, stretch, and store! How is that for "alternative technology"?

Sgt. Pepper of Texas

We're glad to see some of our readers working imaginatively to solve this problem of storage. Perhaps the folks at Readers Digest would be interested as well.

How Do Inmates Do It?

Dear *2600*:

Got a couple of newspaper clippings for you. What I'd like to know is how the county jail inmates got ahold of all those long distance codes. I just can't picture an Apple II with autodial modem attacking a dial-up node from a jail cell.

The Hooded Claw

They didn't need one. All they need is human contact with the outside world.

(continued on page 22)

BLV facts

(continued from page 11)

length of the call (in minutes), and the 1.00 is the charge for the interrupt. The format may be different, depending upon your area and telephone company.

Verification seems to be on a closed network, only accessible by the TSPS. However, there have been claims of people doing BLV's with blue boxes. I don't know how to accomplish BLV without the assistance of an operator, nor do I know if it can be done. But hopefully this article has helped people understand how an operator does Busy Line Verification and Emergency Interrupts.

social interaction with phones

by Dave Taylor

An interesting thing has been happening to our telephones throughout the world—they've been transitioning from being a person-to-person communications device to being a full-blown information provider.

Consider, without leaving my chair I can not only call up people I know (the easy part) but I can also track down people by dealing with information (obtaining their addresses as well as their phone numbers), get stock quotes, my horoscope, the racing results, summaries of the latest installments of various popular television series but, much more interestingly, can actually meet *new* people too.

The phone has been extended to be the ultimate in safe social interaction systems—with the rallying cry of "profit" the phone company and the FCC has been licensing not just 976 numbers, but also is now offering 900 service with a vengeance.

[976 numbers, for those that don't know, are a special class of phone numbers leased to individuals for just about any legal purpose. The person calling is charged typically a connect cost (usually about $1.75) and then a per-minute charge too. The phone company pockets a significant percentage of this revenue, and the owner of the specific service gets the rest. A 900 number is similar to an 800 number (e.g. the toll free phone number area code) but the caller is charged a flat $.50 per call to access it. The numbers operate throughout the continental US and the person who owns the equipment pockets 5 cents for each call placed.]

Somewhat surprisingly, though, I was in England and France a while back and noticed that they're catching on there too! There are big colorful adverts all over the Tube in London advertising a teen party line, for example.

What's also interesting is that not only do they have "call a recording" systems (also known by the name "dial-a-pom" due to the prevalence of that type of recording being available) and systems where you can call up and leave a "personal ad", also hearing someone else's (randomly), but it's been extended to party lines, like they had in the early days of telephones.

A friend of mine runs a 976 "chat" line system: he leases 12 phone lines from the phone company and people calling can connect to up to twelve people all in one big conference call. (There are some built in limitations on the system—by law—they all must terminate within 3 seconds of connect and by technology—boosting the limit to go to more than four or five other telephones makes it sound awful!)

I think that this development is significant for a number of different reasons above and beyond the further utilization of the telephone, however. It's also an excellent example of the sometimes insidious growth and encroachment of technology on our everyday lives.

But most of all, it makes a rather strong statement on the social lives of people in our fast paced society.

I've sat with my friend as he listens to his own line, or calls other lines to hear how they sound, and most of all I'm struck with the tones of despair and loneliness that all the callers seem to have. Underneath their babble (and indeed it's surprising that people pay so much to say so little) is a group of people who are fundamentally unable to succeed socially in our society.

I know of a woman, quite attractive, personable, and fun to spend time with, who has used the 976 personals recording numbers to meet men. She's actually enjoyed spending time with the people she's ultimately met in person, but they all seem to vanish within a week or two.

Yet another person I know claims that his only friend he has that he hasn't met through "phone conferencing", and that he finds it so difficult to make friends at parties and such.

So, in a rather circuitous way, I wonder if

(continued on next page)

social interaction

(continued from previous page)

we're not seeing the usage of these new phone services (and they are used an astounding amount, in excess of a billion dollars worth of phone revenue per year in the US) as indicative of the gradual changes that are transforming our culture and society.

In some sense, they're a direct parallel to computer bulletin board systems—a few years ago when they started to become popular a group of people sprung up that used them as their primary place for making new friends. The parallels are really quite striking. (And the current computer conference systems, like the USENET, are an outgrowth of these early BBS's too, with similar demographics.)

The other question that arises, and I believe is the crux of all of this, is *where did this clique come from?* Is it a new group of people, these that use technology as a vehicle for social interaction, or is it a natural outgrowth of other factors?

My suspicion is that it's an unsurprising result of the expansion of media and the consequent strengthening of the media's "perfect person".

The expectations in society really have changed quite dramatically in the last few years I believe. One must either be part of the popular culture (e.g. the so-called media stereotypes) or they will have a difficult time succeeding socially.

As Clive Barker (director of the new film *Hellraiser*) says in the magazine *Sight and Sound* [a minor character in the original has been turned into the second lead in the adaptation and polished up as a more or less conventional heroine] "I liked the fact that in the novella the girl was a total loser. You can live with someone like that for the length of a novella. You can't for a movie."

What exactly is this saying about our culture?

I've strayed a bit off the beaten path, but I would be most interested in hearing about other people's thoughts on this, especially those outside of the United States.

Roman Hackers

The following article is another in a series of overseas tales of hacking and phreaking.

by Hal from Rome

I have seen that sometimes you give space to foreign contributors, so I hope to tell you some things that could be interesting.

In Europe we still have the pulse dial system and in Italy we probably have the oldest telephone system in Europe. In my country we make every effort to be compared with the rest of the world. So even if we do have a bad telephone organization, we miraculously have a lot of services and our fantasies make up for the faults of the Government.

We have successfully created a good organization of people who use a modem and through this organization we successfully hack a lot of things.

First of all, as described in the May 1987 issue, we learned how to easily call free from the phone booths, first using a little tool (an electric wire) and then without any tools—simply by hanging the handset up quickly, thereby "unlocking" the line for calling everywhere. Unfortunately our company locked all of the booths in July so we're trying to find another way.

We are also able to use "black boxes" when receiving a call. If someone calls, you can switch on this electric box connected to the line, lift up the receiver and talk while the phone is still "ringing". In this case the person who has called you doesn't pay anything because this box makes the telephone exchange believe that you *didn't* lift the receiver. So the exchange believes the telephone in your house is still ringing! Sometimes you may have to put up with a light "ring" while you talk. On local calls you can talk as long as you want because the phones can ring forever. On "extra local" calls (we call them "extra urban" calls), the line will be cut after three minutes and you will have to dial again.

Hacking via Modem

We also have a network for long distance calls via modem. While the United States has Telenet, Tymnet, etc., we *fortunately* have only one network because the telephone system is controlled by the Government. Our network is called "ITAPAC" and, as you can imagine, once you get a password to use it you can call all of the biggest computers in the world (BIX, DIALOG, COMPUSERVE, etc.) and only spend money for a local call.

We have several of these passwords and we're quite sure they won't change soon because they

(continued on page 20)

2600 marketplace

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.

TAP BACK ISSUES. Complete set, vol. #1 to and including vol. #91, including schematics and special reports. Copies in good to excellent condition. $50.00, no checks, includes postage. T. Genese, 219 N. 7th Ave., Mt. Vernon, N.Y. 10550.

DOCUMENTATION on electronic and digital switching systems and PBX's. Willing to purchase/trade. Also looking for other paraphernalia such as Bell System Practices. Write to Bill, c/o 2600, P.O. Box 752C, Middle Island, NY 11953.

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

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

SUMMERCON '88—coming to NYC. Watch this space for more info.

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

FOR SALE: Ex-Bell blue boxes, old and stylish, may even work! Also a wide range of old Bell comms equipment. Call (514) 393-1840 and ask for Rick for details.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

2600 MEETINGS. Fridays from 5-8 pm at the Citicorp Center in the Market (lobby where the tables are)—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for more info.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses. Address: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label.

Deadline for Spring issue: 2/15/88.

Roman Hackers

(continued from page 18)

belong to the telephone company! Strange but true: in Italy it is easier to find passwords that belong to the telephone company instead of hacking private passwords. This is because our telephone company (called "SIP") doesn't believe there are very many hackers and so it doesn't care too much about keeping their passwords secret!

Now using ITAPAC, I very often use systems in the United States and one of my favorite ones is an outdial system—one that you can call and say, "OK, now dial this number in the USA." So using this outdial I can connect to every number via modem in the United States and I can join a lot of BBS's normally not connected on the network.

I hope this is of interest to those of you in the United States. Please contact me on BIX (write to "capoccia" and if you want I can give you my password for a while so you don't have to spend anything and so we can write to each other) or write me a number of a BBS at which I can reach you.

In Italy, there isn't actually *any* law against hackers, so you can use this information as you want. I'm not afraid at all and you can publish my address.

Hal (from Rome)
c/o Enrico Ferrari
Via Giuseppe Valmarana 43
00139 Roma
Italy
Phone 011-39-6-810761

Because of existing laws in the United States and because we are always wary of overconfidence, we have omitted any references to specific hacking on specific systems.

More Long Distance Unpleasantries

Recently I decided I wished to have legal access to a long distance carrier's facilities, so I began to gather toll-free 800 customer service numbers to the major interexchange carriers that served my area. A quick call to 800 DA got me the correct number to US Sprint Customer Service for my area (8005314646), and the correct number for ALC Communications, otherwise known as Allnet (8005210297). I then called US Sprint and inquired about getting a travelcard, or a code on one of their 950 or 800 access numbers. However, the person who answered the telephone was insistent upon trying to get me to sign up with US Sprint as my equal access carrier. I didn't want Sprint as my equal access carrier. But one of their travelcards would cost me $10 a month plus charges incurred if I didn't choose them as my Equal Access carrier. I didn't want to have to fork over this ridiculous charge just for a simple code which could be hacked for free. They lost a prospective customer by being so stubborn about getting my Equal Access dollar (this is understandable, as Sprint has invested a huge amount of money in their Equal Access campaign). Another bad point concerning US Sprint is the fact that its authorization codes have been widely abused and posted on electronic bulletin board systems, where they are then spread to more and more people who are potential abusers. I rarely saw an MCI code, or an ALC code posted on a BBS, and when I did, they went bad very quickly, especially in the case of Allnet. This is due to ALC having the city name of the general area that you called from included in their records. When calls come from different points at the same or close to the same time in excess, the customer can be contacted and the code changed. Anyway, back to the pushy representative: I hope this experience opens the eyes of any potential US Sprint customers. Oh, and incidentally, GTE, which owns US Sprint, is a nuclear weapons contractor with the government. Another bad point (see *2600*, March, 1987).

Next, I decided to try MCI. A quick call to 800 DA revealed their 800 customer service number to be 8006246240. I knew this number was incorrect. I recognized the 624 exchange as the one where MCI had a node, which was 8006241022 and has since been replaced with another 800 number (8009501022) that belongs to MCI and also receives ANI (the phone number you're calling from) when you call it (see *2600*, July 1987). Anyway, I then decided to get "assistance" from a local Bell TOPS operator, who was quite friendly, and completed several calls for me in an effort to find the right customer service number. The TOPS called 800 DA for me and I requested any other numbers they might have for MCI, explaining that the number they had was no longer valid. They gave me a number

more long distance horrors

listed as 'MCI Sales', which was 8006242222. The TOPS (who did not disconnect) then dialed KP FWD+8006242222+ST in an attempt to reach MCI Sales. This number was answered by a Bell ONI Intercept Operator (an intercept operator who didn't know the number I was calling; I had to verbally tell it to her). She then told me that the new number was 8004442222. So, after three attempts, I finally received the correct number for MCI Customer Service, or so I thought. I called this number and informed them of the trouble I had in getting the new customer service number, and the woman who answered the phone said she would look into it. I wonder why AT&T was so slow in getting the new customer service number for one of their major competitors? Updates to the 800 Directory are supposed to be handled automatically, by computer. It seems that someone put a low priority upon this particular company, as I had no problem with any of the others. Anyway, I then began asking the woman some general questions about their service, and only when she asked me my area code was I told that I needed to talk to the Southwest Division, reachable at 8004441212. So, after all this hassle, I finally called and had a chat with what sounded like a Japanese-speaking person who sounded intoxicated. I learned several interesting things from talking to this person. One such thing is that MCI Customer Service reps have access to rate information via a computer. They enter the originating NPA-NXX, and the terminating NPA-NXX, and the computer displays rate information for all three rate classifications (day, evening, and night/holiday). I also discovered that to get a travelcard with MCI, you usually have to pay a one-time fee of $10.30, but they had some sort of special going where you could get the travel card free at this specific point in time. I also asked about MCI operators, assuming that they would be implemented shortly. The man told me they would be there by the end of 1987. This was all fine and well, but it would then take them 10-14 working days to activate my service. I found out other interesting things about them that I plan on including in a separate article which will be released at a later date. One last bad point about MCI—they, like GTE, are a nuclear weapons contractor (see *2600*, March, 1987), so I decided not to deal with them.

The next carrier up was Allnet, or in truth, ALC Communications (formed when Allnet merged with Lexitel). However, 800 DA didn't have any listing for ALC Communications, but they did have a number for "Allnet Customer Service". I called this number and the telephone was answered by a new employee. This person was very helpful and answered all of my questions with no hassle. Allnet had no monthly surcharge for the use of a travel card, and they did not try to push me into signing up with them as my Equal Access carrier. So in other words, I was able to get a code on Allnet easily without much hassle. From the three carriers I sampled, Allnet was by far the most helpful. If you are thinking of getting your own travelcard, I would suggest Allnet. They are, of course, a major reseller of other companies' lines. That is to say they do not have their own network like MCI or US Sprint. Thus, you will have to put up with slightly lower quality lines, but they are still more than adequate for voice and data transmissions.

When choosing, be sure to compare the long distance services that are available in your area before you decide to pick one. Ask them questions, but don't be rude. MCI in particular has their customer service numbers set up in their own 800 exchange, and calls to this exchange will receive ANI. So being polite and tactful is advisable when dealing with them from a home telephone.

Also keep in mind that the customer service numbers listed here are for my area code. You will have to get your own numbers for your area code if you wish to engineer these companies.

One last note: readers, share your experiences! Only through an intelligent communications forum like *2600* can we inform each other and the general public of the good/bad aspects of telephone systems here and abroad.

SOME NUMBERS

10041-1-700-777-7777	ALLNET conference line in NY – $1 a minute
10220-1-700-611-6116	Western Union Help Line
1-800-988-0000	Western Union Long Distance Customer Service
1-800-988-4726	Western Union Telegram Operator

(continued from page 16)

DECEMBER'S LETTERS

Guards can prevent visitors from bringing in knives and guns, but so far they've been unable to keep people from reciting numbers. Someone could also easily set up a voice mailbox to read out this month's Sprint codes. All an inmate has to do is call that number and write down the codes. But isn't it true that all calls from a prison have to be collect? That's no problem—simply make the first part of the voice message say "Sure, I'll accept" or something similar.

BBS Thoughts

Dear *2600*:

First off, I'd like to compliment you on your magazine. It really shows how little the average person knows of what's happening in our techno world. Secondly, I saw your comment about wanting to set up a network of safe BBS's. Just in time—I was thinking about re-opening mine, yet abhor the thought of running a pirate BBS again (as in software hacking). I'd love to run a "2600 authorized BBS". I would be running on an Amiga 1000, 3½ inch drive, and 300/1200 BPS. It would be 24 hours a day. I'm still looking for the right software to run, but any that I choose would easily meet your requirements.

P.A.Z.

We have some additional requirements that we can go over with you at a future date. We expect to start adding new boards sometime in January. Anyone else who's interested in running a 2600 board should contact us.

The Missing Chip

Dear *2600*:

As per the "lost" 8038 chip for the box plans: ICL8038 precision waveform generator voltage cont. oscillator, made by Intersil—now GE/RCA and available from the "common" distributors in most cities (i.e. Arrow Electronics, Schweber Electronics, Hamilton/Avnet Electronics) or to the "hobbiest" from Jameco Electronics, 1355 Shoreway Road, Belmont, CA 94002, (415) 592-8097, FAX 415-592-2503, Telex 176043 (ICL8038CCJD $3.95 w/$20 minimum order).

Yet Another Telco Ripoff

Dear *2600*:

Have you ever been talking on a payphone and had your time run out? First the phone collects your money and then the nice man asks you to deposit a nickel for another five minutes. You reach into your pocket and all you have is a quarter. You deposit your quarter and are left alone for only another five minutes! It seems quite unfair that no matter what you deposit is treated as a nickel. I can understand that under primitive central office equipment the phone just checks to see if there is a coin ground. But today since most big cities have a majority of their central offices cut over to ESS, why can't someone at the phone company modify their switches to accept dimes as dimes and quarters as quarters?

Mary M.
Cornland, Iowa

Why indeed? Let's hear some "explanations" for this one from the folks on the inside. If we don't get a satisfactory answer, you may be looking at next year's project to combat consumer fraud.

The correct address to send a letter or to forward an article is:
2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953

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 to arrange an upload. Send US mail to

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

CONTENTS

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

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

WARNING:
MISSING LABEL