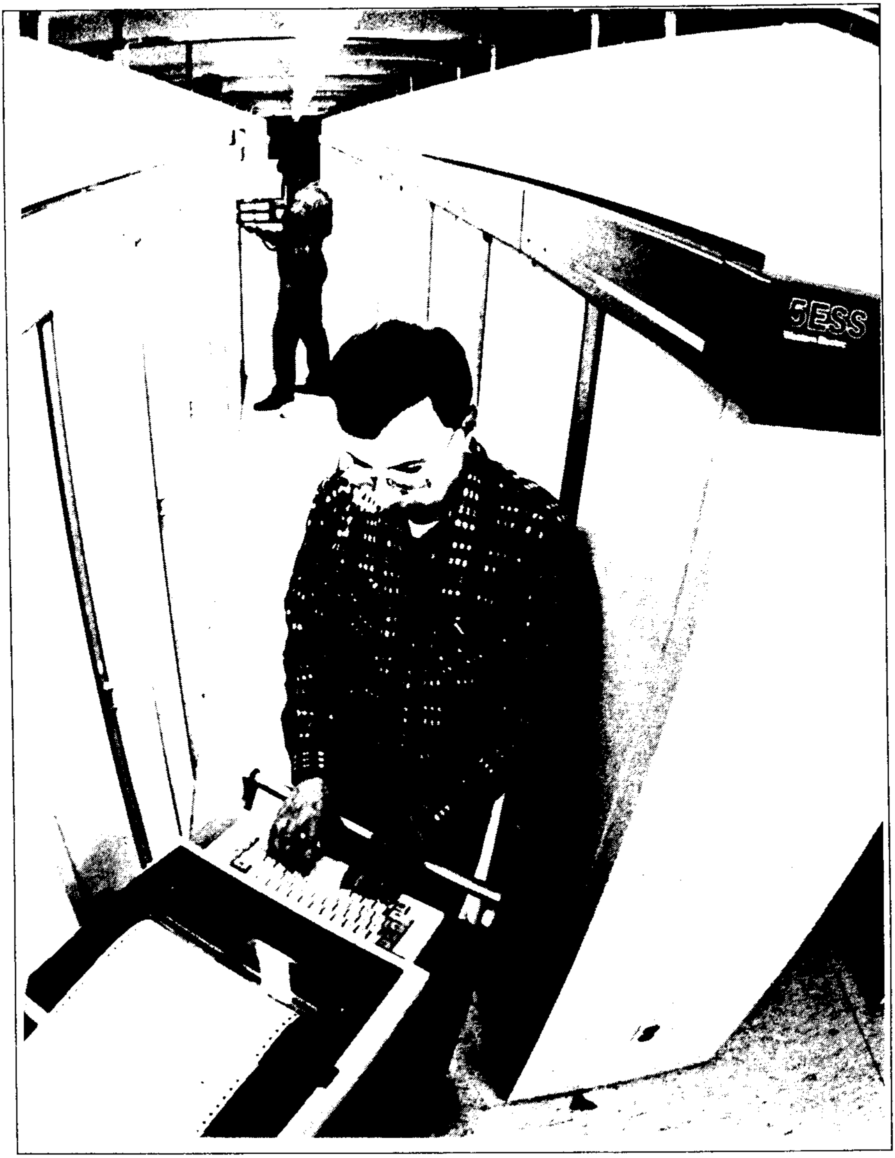
2600

The Monthly Journal of the American Hacker

Volume 4, Number 11 November, 1987 $2



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 U.S. mail to

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

We now have several ways of staying in touch with the rest of the world. As promised, the first official bulletin boards of 2600 Magazine are now online with more on the way.

We're quite happy with what we've started out with. The two boards are both in area code 914, just north of New York City. Board #1 is the legendary OSUNY, a BBS that has been talking about phone phreaking and computer hacking for longer than any other board that we can remember. In fact, OSUNY is mentioned on the very first page of our very first issue. And it's also been referred to in Newsweek, although not very accurately. Board #2 is the Central Office, another well known bulletin board for hackers and phreaks. We're proud to be affiliated with these boards and we'd like to ask anyone else interested in running a 2600 board to log onto these first so you can see what a 2600 board is all about.

As we've stated previously, these boards are completely open to whoever calls in. No area is off limits or for "elite" users only. There are no areas of

(continued on page 10)

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Bobby Arwatt

Cover Art
Ken Copel
Tish Valter Koch

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

Production: Mike DeVoursney.
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 (OSUNY): 914-725-4060
BBS #2 (CENTRAL OFFICE): 914-234-3260
USENET ADDRESS: 2600@dasys1.UUCP
ARPANET ADDRESS: phri!dasys1!2600@nyu

HACKING IBM'S

by Lex Luthor
and The Legion of Hackers

Introduction

IBM mainframe computers make up over 50 percent of the mainframes used today in the United States. These systems are traditionally used in industries such as insurance, banking, universities, and so on. For some reason, IBM systems as a whole have not been very popular with hackers. This may be due to the complexity of the operating systems run on IBM systems compared to others such as UNIX or VMS. Another reason may be that there is much variety from shop to shop. IBM systems are more commonly modified and customized to fit an individual corporation's needs and the lack of "universality" for commands, files, programs, and other procedures makes it difficult to attempt to use without any type of specific documentation. The lack of detailed on-line help also hinders the hacker. I believe that the VM/CMS Operating System is by far the best and easily learned of the IBM systems. But compared to other Operating Systems like UNIX or VMS, VM/CMS is cumbersome and harder to learn.

Acronyms

Before I even attempt to start this article, I will list the IBM-specific acronyms we will be using and some others that you may find on various IBM systems. I list them here so I will not have to do it throughout the article. If you need to know what one of them means later, just refer back to this list.

VM/SP: Virtual Machine/System Product
CP: Control Program
CMS: Conversational Monitoring System
HPO: High Performance Option
VSE: Virtual Storage Extended
MVS: Multiple Virtual Storage
TSO: Time Sharing Option
JES: Job Entry System
CICS: Customer Information Control System
VSAM: Virtual Storage Access Method
VTAM: Virtual Telecommunications Access Method
IX: Interactive Executive
IPL: Initial Program Load
IVP: Installation Verification Program
RSCS: Remote Spooling Communications Subsystem
DASD: Direct Access Storage Device
EREP: Environmental Recording Editing and Printing
SNA: Systems Network Architecture
NCCF: Network Communications Control Facility
REXX: Restructured Extended Executer Language
VTOC: Volume Table Of Contents
DOCS: Display Operator Console System
JCL: Job Control Language
ACF: Advanced Communications Functions
SQL/DS: Structured Query Language/Data System
DBA: Data Base Administrator
GCS: Group Control System
SCP: System Control Program
FDP: Field Development Program
CNA: Communications Network Application
POF: Programmable Operator Facility
PSW: Program Status Word
SSCP: Subsystem Services Control Point
IPCS: Interactive Problem Control System
DCSS: Discontiguous Shared Segments
VMCF: Virtual Machine Communications Facility
FIFO: First In First Out
LIFO: Last In First Out
AP: Attached Processor
MP: Multi-Processor
R/D: Read/Only
R/W: Read/Write

Logging In

Typically, when you come across a system running an older version of CMS, it will respond with:

```
VM/370 ONLINE
!
```

This message is somewhat of a contradiction. The majority of VM/CMS systems are rarely run on actual 370 systems but on other processors, such as the 43XX series and the 30XX series.

The period "." prompt is the surest way of verifying that you have indeed connected to a VM/CMS system, aside from the "VM/370 ONLINE" message which is usually printed. This prompt should not be confused with DEC's TOPS-10 system, which also has the prompt of a period. Newer versions will give you this menu:

```
Enter one of the following commands:

LOGON userid (Example: LOGON VMUSER1)
DIAL userid (Example: DIAL VMUSER2)
```

VM/CMS

MSG userid message (Example: MSG VMUSER3 GOOO MORNING)
LOGOFF

This menu may vary from system to system, since system managers may opt to omit commands from the menu or add others. When hacking a system, this menu will appear before you can attempt to login, thus becoming very tedious and time consuming especially at 300 baud as you have to wait an etemity for each logon attempt.

> *"Compared to other operating systems... VM/CMS is cumbersome and harder to learn."*

Other responses after connecting are "Ready to Host", "Press break key to begin session" and "Invalid Switch Characters". The last response is commonly found on Telenet and other packet switched networks, in which you may have to specify "VM" for a VM/CMS system, or "TSO" for an MVS/TSO system. There may be other IBM systems to select from, or "VM" may not be a valid system. You may also have to specify "LOGON VM" or just "LOGON" before the port selector connects you to the host system.

LOGON can be abbreviated as just "L". A userid can be from 1-8 characters in length, but the first character *must* be a letter (in most systems you come across this will be true, but due to customization of systems, it's possible this and even the 8 character password limit may be extended). A typical logon may look like:

```
.L COMOSOLO SYSGUESS NOIPL
```

"." is the system prompt, L is the LOGON command, COMOSOLO is the userid, SYSGUESS is the password, and NOIPL is the only 'login qualifier' allowed for the VM/CMS system. NOIPL specifies that the IPL name or device in the VM/SP directory should not be used for an automatic IPL. IPL simulates the LOAD button and the device address switches on the real computer console. Basically it "boots" your part of the CMS system. This is another different concept. A user can boot (or crash) their part of the system, not the whole system (in most cases). NOI`L would be used when a system dumps you into a program which allows you little or no mobility such as a restricted menu of options (i.e., a system backup utility) and logs you off without gaining access to CMS. NOIPL will prevent this program from running if it is listed in your automatic IPL entry within the CP directory. This should allow you access to the system. Otherwise the program was specified to run within your PROFILE EXEC which lists things to be done upon logon. NOIPL is somewhat similar but not identical to the login qualifier "/NOCOMMAND" for DEC's VAX/VMS systems.

If the Password Suppression Facility is installed on the system, you will receive an invalid format message whenever the userid and password are entered on the same line. This is obviously a security measure to prevent users from entering their password in full view of anyone who may be watching as the password is not "masked". Thus, you will have to enter your password on a separate line when the system prompts you for it. The advantage of entering the userid and password on one line (especially at 300 baud) is that you can try more userids and passwords in a shorter period of time while still availing yourself of the system's generosity of informing you when an invalid userid has been entered.

Error messages

There are various error messages one may encounter while logging into a VM/CMS system. The ones you should be most concerned about are:

Userid not in CP directory. When an invalid userid has been entered, you will receive this message. This indication gives the hacker a distinct advantage for gaining entry to the system. Probably the largest security hole in any system comes from telling the user when a valid username has been entered. After all, obtaining a valid userid is half the battle. The other half is obtaining a valid password. Even the weakest operating systems no longer give an indication of when a valid ID has been entered. Why IBM has not changed this is a mystery to me.

When a valid userid is entered you will be asked to enter a password if you did not already do so. If the password is correct, the system will attempt to log you on. If not, you will receive one of two messages:

(continued on page 16)

US Social Security Prefixes
from The Disk Jockey

001-003	New Hampshire	440-448	Oklahoma
004-007	Maine	449-467	Texas
008-009	Vermont	468-477	Minnesota
010-034	Massachusetts	478-485	Iowa
035-039	Rhode Island	486-500	Missouri
040-049	Connecticut	501-502	North Dakota
050-134	New York	503-504	South Dakota
135-158	New Jersey	505-508	Nebraska
159-211	Pennsylvania	509-515	Kansas
212-220	Maryland	516-517	Montana
221-222	Delaware	518-519	Idaho
223-231	Virginia	520-	Wyoming
232-236	West Virgina	521-524	Colorado
232-232	North Carolina	525	New Mexico
237-246	North Carolina	585	New Mexico
247-251	South Carolina	526-527	Arizona
252-260	Georgia	600-601	Arizona
261-267	Florida	528-529	Utah
589-595	Florida	530	Nevada
268-302	Ohio	531-539	Washington
303-317	Indiana	540-544	Oregon
318-361	Illinois	545-573	California
362-386	Michigan	602-626	California
387-399	Wisconsin	574	Alaska
400-407	Kentucky	575-576	Hawaii
408-415	Tennessee	577-579	Washington DC
416-424	Alabama	580-584	Puerto Rico
425-428	Mississippi	596-599	Virgin Islands
587-588	Mississippi	586	Guam, Samoa
429-432	Arkansas	700-728	Railroad
433-439	Louisiana		

Some numbers are shown more than once because they have been transferred from one state to another or have been divided for use among certain geographical locations. No new 700-series railroad numbers have been issued since July 1, 1963. These are used by credit agencies and other services when verifing birthplace, tracking down individials, or for use in creating new identification.

listening in: catch me if you can!

by The LNA Master

Are you tired of watching scrambled video from HBO and the Movie Channel, etc.? And you don't want to watch Dr. Gene Scott or Jerry Falwell or any of the other TV preachers? Do you feel your satellite dish is going to waste? Well, here's something fun you can do with it.

In addition to receiving video and audio signals, your satellite dish can be used as a wiretapping device. Yes, some of you can actually wiretap from your own living room—a fact you probably didn't know. Wiretapping is illegal, but as the title of this article says, catch me if you can. It's virtually impossible to detect this particular brand of listening in.

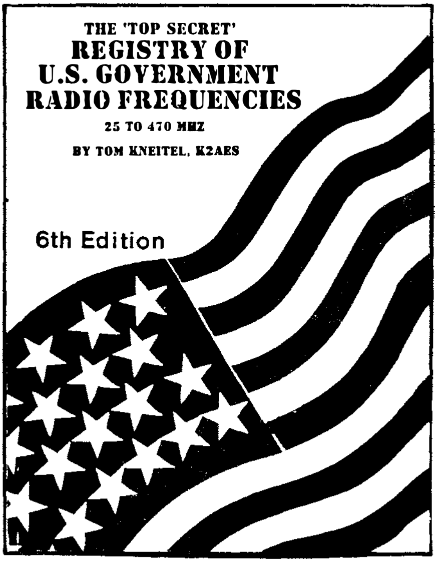
All you need for this project is your basic home satellite dish antenna, also known as TVRO or televison receive only. What you need to do is tum to the AT&T satellite known as Telstar 301. You'll notice between Channel 20 and 23 (that is, Channel 21 and 22) you'll see a blank screen as if there were a station there. You won't hear anything except maybe an occasional garbled sound.

This is what you do to listen in on phone calls. Take a general coverage shortwave receiver (covering between AM broadcast band and 30 megacycles). Connect the antenna input of your shortwave to the video out terminal on your satellite receiver. Tune the shortwave receiver on lower side band (LSB) anywhere between the broadcast band (1.6 megahertz) and 7.5 megahertz. Make sure your satellite receiver is either on Channel 21 or 22. You will pick up more calls to Hawaii, Puerto Rico, Alaska, and the Caribbean than you ever thought possible. Who would have dreamed there would have been that many phone calls to listen to? About every 3½ kilohertz there is a phone conversation. If you do not hear a phone conversation, you will hear a continuous tone of 2600 hertz. Tune your receiver to where you believe 2600 is coming in perfectly, then listen for a click followed by MF (blue box) tones followed by a ring. You will then be able to listen in on AT&T calls to area code 808, 809, and 907.

For frequencies above 4.1 megahertz, switch to upper side band (USB). Also, you can tune in Channel 8 of Telstar 301. It appears that Channel 8 on your standard satellite receiver box switches to the US Sprint service from the mainland to Hawaii. Sprint codes can be (and have been) gotten successfully by listening to the calls. Interesting conversations are all over the place, such as the man from Long Island who has two wives and was promising the second wife over the phone that she could stay in his house in Hawaii until he "got rid of" wife number one.

Telstar 301 can be found at 96 W on the satellite dish. Spacenet 2, which is located at 69 W is all US Sprint. Domestic calls as well as overseas calls can be monitored.

Other interesting satellites are ASC1 at 128 W, Westar 2 at 79 W, and Comstar D4 at 76 W. On these, simply tune across until you hit a blank channel that looks like it's carrying a signal. Then tune the shortwave receiver anywhere between 1.6 and 7.5 megahertz. If the conversation doesn't straighten up, switch to LSB or USB on the shortwave.



THE 'TOP SECRET'
REGISTRY OF
U.S. GOVERNMENT
RADIO FREQUENCIES
25 TO 470 MHZ
BY TOM KNEITEL, K2AES

6th Edition

A Review of "The 'Top Secret' Registry of U.S. Government Radio Frequencies"

by Mr. Icom

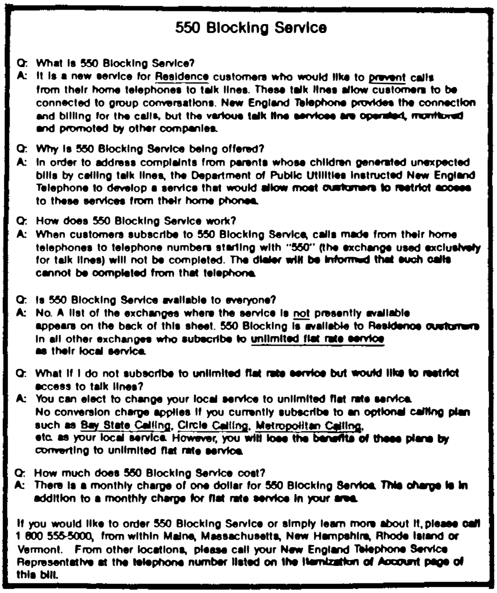
Scanner listening seems to have a certain mystique amoung phreaks and hackers, particularly in regards to listening to mobile/cordless/cellular phones, and certain govemment agencies. However, unlike mobile phones, whose frequencies are well known, the feds' frequencies appear to be hidden away from

(continued on page 22)

the telecom informer

BY STAFF

They've done it again. This time, after repeatedly and aggressively promoting their 550 talk line numbers (phone numbers beginning with 550 that connect callers to total strangers), New England Telephone has devised a plan to block access to these numbers from your home -- for a monthly charge. This is supposed to benefit those people who listened the first time and called all those numbers in the advertisements, winding up with an incredible bill. Now that they've been given a taste of what kind of "accidents" their phones can have, a dollar or two for "insurance" isn't so unreasonable. Where have we seen this before?....New Jersey may soon have talking yellow pages. Using a touch tone phone, subscribers will be able to call a computerized system, enter a four-digit number, and listen to a recorded message containing theater events, stock market reports, and anything else you could possibly want. The service will be free to customers. To advertise on it will cost about $80 a month....In Annapolis, Maryland, a man pleaded guilty to stealing long distance telephone service using his home computer, which the judge ordered destroyed. An intelligent man....While MCI and US Sprint are trying to grow and recover from their losses, AT&T is trying their best to knock them out. AT&T has started a new program for COCOT (Customer Owned Coin Operated Telephone) companies. The contract for this program insists that payphone companies route all their long distance traffic through AT&T. The companies receive between 3 and 17 percent commission depending on how much long distance usage there is. The contract also states that the phones cannot process Visa or Mastercard calls (many COCOTs now have a magnetic card reader installed), and goes on to say 950 and 10xxx calls are not allowed unless the payphone tariff requires them in that state. An interesting note: in New York State the only rules governing COCOTs are 1) they must give free 911 service; 2) they must give free local directory assistance or have a phone book nearby (a book in the same building counts!); and finally 3) either on or around the phones there must be a number for service or complaints....MCI is expanding International Direct Dialing. As of September 15, Israel was MCI's 58th direct dial country. They will lease equipment from AT&T to facilitate long distance service to another 140 countries....US Sprint now provides access to over 60 countries, while only about 20 are dialable with a FON card (Sprint's calling card service). The rest of the countries are only dialable with 1+ service. Among the countries not dialable by calling card are Argentina, Chile, Dominican Republic, Hong Kong, and Taiwan. (As of November 7, US Sprint suspended international calls to the Dominican Republic from area codes 212 and 305.) US Sprint says by the end of the year they should handle over 80 countries....MCI will offer operator service in 1988 so that customers can use calling cards from a



550 Blocking Service

Q: What is 550 Blocking Service?
A: It is a new service for Residence customers who would like to prevent calls from their home telephones to talk lines. These talk lines allow customers to be connected to group conversations. New England Telephone provides the connection and billing for the calls, but the various talk line services are operated, monitored and promoted by other companies.

Q: Why is 550 Blocking Service being offered?
A: In order to address complaints from parents whose children generated unexpected bills by calling talk lines, the Department of Public Utilities instructed New England Telephone to develop a service that would allow most customers to restrict access to these services from their home phones.

Q: How does 550 Blocking Service work?
A: When customers subscribe to 550 Blocking Service, calls made from their home telephones to telephone numbers starting with "550" (the exchange used exclusively for talk lines) will not be completed. The dialer will be informed that such calls cannot be completed from that telephone.

Q: Is 550 Blocking Service available to everyone?
A: No. A list of the exchanges where the service is not presently available appears on the back of this sheet. 550 Blocking is available to Residence customers in all other exchanges who subscribe to unlimited flat rate service as their local service.

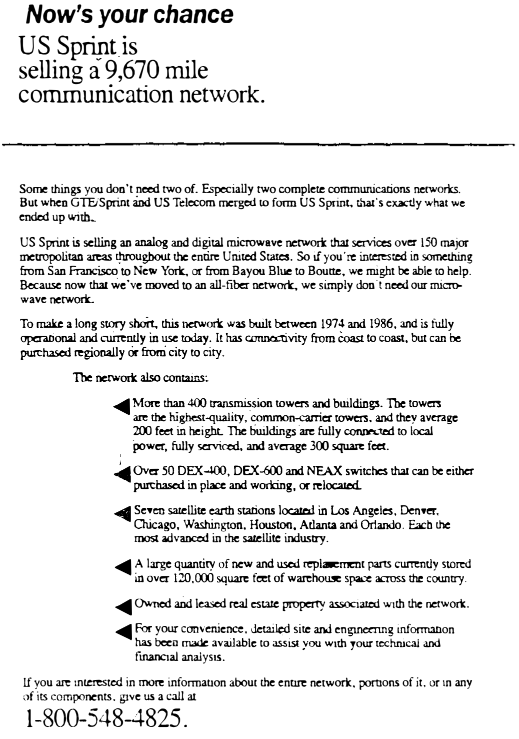
Q: What if I do not subscribe to unlimited flat rate service but would like to restrict access to talk lines?
A: You can elect to change your local service to unlimited flat rate service. No conversion charge applies if you currently subscribe to an optional calling plan such as Bay State Calling, Circle Calling, Metropolitan Calling, etc. as your local service. However, you will lose the benefits of these plans by converting to unlimited flat rate service.

Q: How much does 550 Blocking Service cost?
A: There is a monthly charge of one dollar for 550 Blocking Service. This charge is in addition to a monthly charge for flat rate service in your area.

If you would like to order 550 Blocking Service or simply learn more about it, please call 1 800 555-5000, from within Maine, Massachusetts, New Hampshire, Rhode Island or Vermont. From other locations, please call your New England Telephone Service Representative at the telephone number listed on the Itemization of Account page of this bill.

rotary phone. Once that is established they will also offer collect calls, trouble assistance, and other operator services. US Sprint has provided operator service for a good while now. Just dial 800-332-0777 or for you equal access nuts 103330 (107770 is now extinct)....While both MCI and US Sprint are offering 800 service neither provides 800 directory assistance. Take 800-444-9999, an MCI 800 number owned by Mrs. Fields Cookies—we called MCI and asked them if they had the 800 number for Mrs. Fields. They told us rather matter of factly that the number for 800 directory assistance is 800-555-1212. We tried to explain that *that* number was for AT&T 800 numbers, but were silenced with a click. When we called 800-555-1212, we asked the woman who answered "AT&T 800 information," if she had the number for Mrs. Fields Cookies. She said there was no listing. It just goes to show if you're going to get an MCI 800 number, you have to advertise or else no one will *ever* call you....With US Sprint's ongoing advertising nonsense about hearing a pin drop over the world's only fiber optic network they neglect to mention that you can also hear one drop on every long distance company—AT&T, MCI, Allnet, ITT, RCI, Western Union (oh well, almost every company). In its continuing quest to cut over to "Network 3" (originally scheduled to be completed by June 27, 1987), US Sprint has sent out notices to old GTE Sprint (950-0777) customers. The 9 digit codes (which started out as 7 digits plus a 2 digit travel code) were replaced by a 7 digit code which can only be used from your home town. Even these new codes were only given out to customers without equal access. Until now when you traveled you could still dial 950-0777 and place a call without a surcharge. Now when you leave your city you must use your FON card and pay a 55 cent surcharge with each call. The letter continued stating that one day soon when you call your access number (for the 7 digit home codes) you will hear a recording giving you a new number. This day has already come. There goes the last bit of GTE Sprint left in US Sprint. And soon they'll be selling their old network (see illustration)....Southern Bell has a new service for Florida residents who travel. Called "The Right Touch Service", this program allows customers to disconnect and reconnect their telephone service via a touch tone phone. From anywhere in the country you can call 800-826-6290 to receive a series of interactive recordings. Callers are asked to enter their telephone number which must be in area codes 305, 813, or 904. They are then prompted for a personal access code. This 4-digit PIN number (not the calling card PIN) was mailed to customers recently. When this service was

(continued on next page)



Now's your chance

US Sprint is
selling a 9,670 mile
communication network.

Some things you don't need two of. Especially two complete communications networks. But when GTE/Sprint and US Telecom merged to form US Sprint, that's exactly what we ended up with.

US Sprint is selling an analog and digital microwave network that services over 150 major metropolitan areas throughout the entire United States. So if you're interested in something from San Francisco to New York, or from Bayou Blue to Boutte, we might be able to help. Because now that we've moved to an all-fiber network, we simply don't need our microwave network.

To make a long story short, this network was built between 1974 and 1986, and is fully operational and currently in use today. It has connectivity from coast to coast, but can be purchased regionally or from city to city.

The network also contains:

- ◀ More than 400 transmission towers and buildings. The towers are the highest-quality, common-carrier towers, and they average 200 feet in height. The buildings are fully connected to local power, fully serviced, and average 300 square feet.
- ◀ Over 50 DEX-400, DEX-600 and NEAX switches that can be either purchased in place and working, or relocated.
- ◀ Seven satellite earth stations located in Los Angeles, Denver, Chicago, Washington, Houston, Atlanta and Orlando. Each the most advanced in the satellite industry.
- ◀ A large quantity of new and used replacement parts currently stored in over 120,000 square feet of warehouse space across the country.
- ◀ Owned and leased real estate property associated with the network.
- ◀ For your convenience, detailed site and engineering information has been made available to assist you with your technical and financial analysis.

If you are interested in more information about the entire network, portions of it, or in any of its components, give us a call at

1-800-548-4825.

introduced a few months ago, customers had 3-digit PINS. It's quite possible that those first PIN's were actually the "account codes", those three numbers that follow the telephone number on the phone bill. With this service, there is no fee to turn off your phone line, but there is a $20.50 charge to turn it back on. Right Touch is available 24 hours a day and has the capacity to handle 26 callers simultaneously. While it may be a handy convenience, we wouldn't be surprised if the service got more abuse than use. Considering the amount of lines in Florida, Southern Bell may have used some sort of formula to assign the PIN's, thereby avoiding the trouble of entering millions of PIN's for their customers. If anyone finds this to be true, give us a call. Sanford Bingham of *CO Magazine* reported that when the service first started, he gave 305-555-1212 as his number. "I gave 999 as my code. Astoundingly it worked. The voice thanked me and began to ask questions." Since then, the system has been programmed not to accept 555, 950, 976, and others as valid exchanges. On a similar note, customers of South Central Bell can dial 1-557-7777, a toll-free number accessible only to local callers, to get billing information, disconnect or reconnect service, arrange for payment, order a duplicate copy of their phone bill or custom calling services, all without having to deal with the business office. (What is left for the business office to handle? Most likely, complaints about this new service.) South Central Bell started this service on a trial basis in early September with 40,000 customers in Kentucky....And finally, we've discovered a marvelous little game you can play with Sprint representatives. If you call 800-521-4949, they'll answer with the following greeting: "Thank you for calling US Sprint. By placing your order today, you will enjoy the clearest sounding long distance calls ever. My name is [name].

(continued from previous page)

How may I help you?" This is one of the longest greetings we've ever heard and we've made an amazing discovery concerning it. If you hit a touch tone in the middle of the greeting, the representative on the other end automatically jumps to the word "Hello?" It's just like an interactive computer! Try it today.

(continued from page 3)

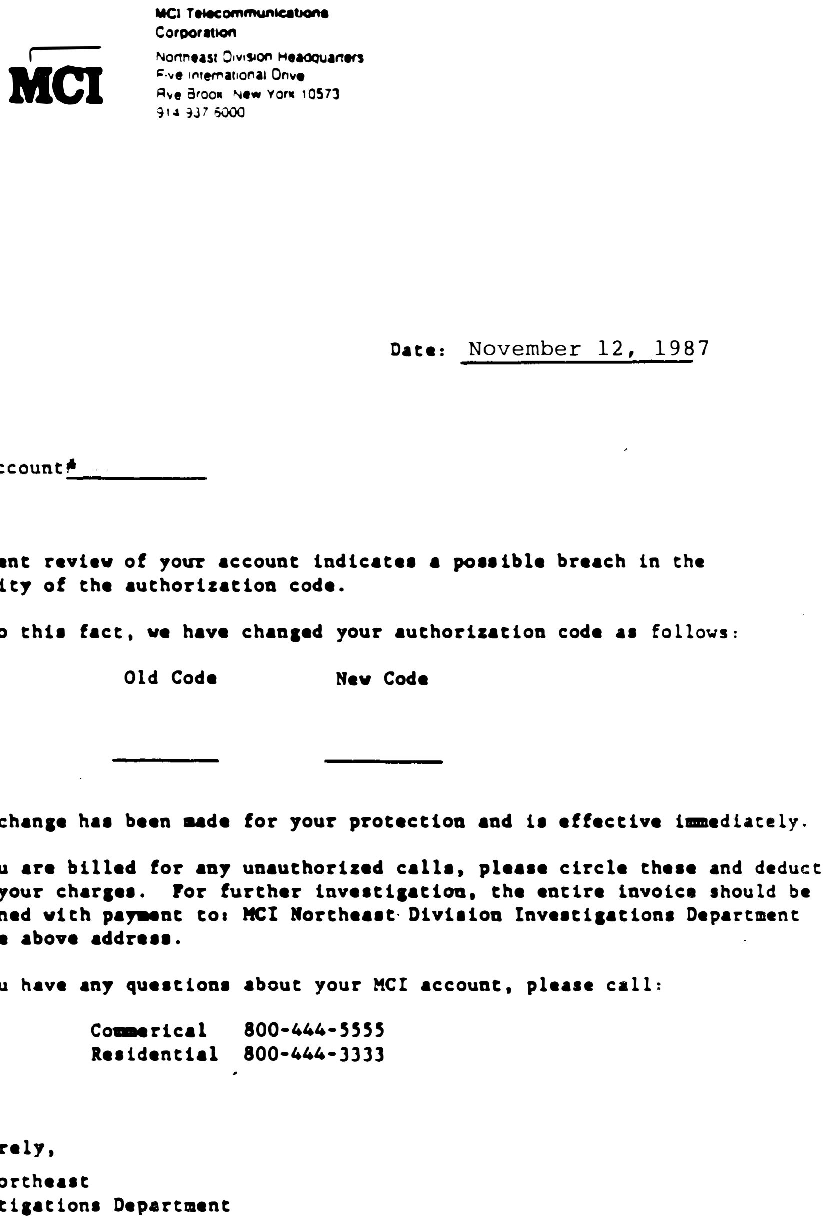
the systems where credit card numbers, MCI codes, or passwords are being posted. But we refuse to put restrictions on users' private mail. Above all else, private mail must remain private. Even the system operator has no idea what is in each user's private mailbox—that's the only fair way to run a system. Of course, it's quite possible that someone will send a Sprint code to someone else through the mail. Or an obscene word. Or a poem. We do not take responsibility for the contents of private mail. And neither does the post office.

Both boards are similar in format. There are a series of rooms to "GOTO". Some of them are obvious, some may take a little guesswork. You can choose the rooms you want to be a part of or even create rooms. Entry is not restricted or monitored, but you do have to know the name of the room you're entering. (This is not hard information to come by, either through guessing or asking around.) Files are also stored in some of the rooms. These are easy to look at and download.

There is plenty of online help available for users. And should you run into a problem of any sort, simply leave feedback or call us at (516) 751-2600. Every 2600 board will have an area for users to leave us public feedback. Both of these boards have a 2600 room. You can use this feature to communicate with other subscribers, offer criticism, praise, and suggestions. Of course, you can also do this privately by sending us mail.

These systems are completely free to use and full of information and

(continued on page 21)



MCI

MCI Telecommunications
Corporation
Northeast Division Headquarters
Five International Drive
Rye Brook New York 10573
914 937 6000

Date: November 12, 1987

RE: Account#

A recent review of your account indicates a possible breach in the security of the authorization code.

Due to this fact, we have changed your authorization code as follows:

Old Code ______ New Code ______

This change has been made for your protection and is effective immediately.

If you are billed for any unauthorized calls, please circle these and deduct from your charges. For further investigation, the entire invoice should be returned with payment to: MCI Northeast Division Investigations Department at the above address.

If you have any questions about your MCI account, please call:

Commerical	800-444-5555
Residential	800-444-3333

Sincerely,

MCI Northeast
Investigations Department

WHY DO THESE LETTERS ALWAYS LOOK SO SLOPPILY WRITTEN? In addition to their inability to spell "commercial", MCI doesn't seem to be able to make our new code work. When we called to find out why, the friendly representative told us that "effective immediately" means 5 to 7 days in most cases. In addition to providing long distance alternatives, MCI now provides logic alternatives. Meanwhile, US Sprint still hasn't gotten around to taking away that $1200 outstanding balance that someone racked up on our account. "Just ignore it," they keep saying. That ought to be their corporate slogan. On our last conversation, they told us that we actually had a $12,000 bill a few months ago which they never sent us since it seemed unusual. And so it goes.

WHY NOT

Double Beepers

Dear *2600*:

Recently you mentioned beeper companies not yet being raided by the police for phone numbers. They don't have to raid them! According to a friend who runs a large beeper company, the authorities can, with a warrant, legally obtain duplicate beeper numbers. Any access to the monitored number also beeps the duplicate number in the police station.

Bob from Los Angeles

How clever. So now we have beeper tapping. But will the beeper companies be as cooperative with the authorities as the phone companies?

Why No Boxing?

Dear *2600*:

In the course of two years of telecom, I've read countless G-files which describe the (virtual) spectrum of "boxes". Yet few files I've encountered give a clear explanation as to why boxing is impossible in electronic switching offices. Would you mind explaining Common Channel Interoffice Signaling (CCIS), and just how an electronic office "prevents" boxing? Thanks.

Franken Gibe
Texas

Put quite simply, it's impossible to use a blue box in an electronic switching office under CCIS because the equivalent of the blue box tones that a phone phreak would send are transmitted over a completely different line. Since you don't have access to these lines, blue boxing no longer works. This is also called out-of-band signaling. For a more thorough discussion, refer to page 2-7 of the 2600 1985 collection, available from us for $25.

Apple Hacking

Dear *2600*:

I thought some of your readers might be interested in the following:

Does your school have a bunch of Apples hooked up to a Corvis? Well, if they do, this is for you.

If you want all the accounts and passwords all you have to do is follow these simple instructions. First when it prompts you for your ID, simply hit ctrl-reset a few times. You should now have an Applesoft Basic prompt. Now type in this one line program:

```
10 FOR I=6281 TO 7252:PRINT CHR$(PEEK(I));:NEXT I
```

Now that you have that typed in, RUN it. The program should dump all of the passwords onto the screen. User names are usually two to four characters long. Passwords are two characters long. Also, disregard any punctuation following a password.

Let's say you had some output that looked like this: "... P1 P2 TYIPXX P3..." The "P1" and "P2" would be user ID's that require no passwords. The "TYIPXX" would be user id "TYIP", password "XX". "P3" would be the same as "P1" and "P2".

That's the basics of Hacking Corvis Constellation. Until next time have phun and hack on.

The Rifter

More How-To Articles

Dear *2600*:

It's been awhile since I've seen an article on boxing. Why don't you run a how-to article—one that addresses international calling procedures? I'm sure you have the capability of coming up with a very informative article on this subject, and many readers would appreciate it.

Tabula Rasa

WRITE US A LETTER?

While we have a number of how-to articles that we've published in the past, we'll be happy to print any new information, including new boxes, calling techniques, etc. International calling and red boxes are at the top of our "wanted" list.

A New Source

Dear *2600*:

I just found a great source for information on news about security and suchlike. It's in a quarterly journal called ACM SIGSOFT, which is the "special interest/software" group of the Association for Computing Machinery. The articles within contain a lot of interesting issues about security and so on, and many are also amusing.

Reading these articles makes me realize how much I miss the news column of your magazine. Though some phreaks and hackers feel this stuff is just fluff and would rather see technical diagrams in its place, I felt it was the best part of the journal. I enjoy reading about VMS tricks to grab passwords, but I also want to know about what's happening in the world out there (other than the latest phreak arrest). Vandal-phreaks cause some damage, but I also find it enlightening to read items like "The FBI estimates the average theft loss from computer frauds at $600,000 [per fraud]," as on page 13 of this July's ACM SIGSOFT.

You might want to mention the existence of this resource as I suspect there are quite a few of us wild and weird news junkies still out there in subscriberland.

E.H.

We still have a news column. It's called The Telecom Informer and it combines all kinds of newsworthy items into one long, rambling article. We'll try to cover as many interesting occurrences as we can for future editions. For readers interested in subscribing to ACM SIGSOFT, write to the Association for Computing Machinery Inc. (ACM), Post Office Box 12114, Church Street Station, New York, NY 10249. Let us know what you find out.

Pen Registers

Dear *2600*:

As I stated in a previous letter, my Radio Shack pen register doesn't record numbers when I use a cordless phone (Phonemate).

It would be interesting to know the make of the pen register and cordless phone that "Worried and Upset in Arizona" uses that does register phone numbers (September 1987 letters page).

Samuel Rubin

Unique Projects

Dear *2600*:

No one makes the following for the Apple:

1. A combination speech generator, clock, printer buffer, and copy card. Maybe even some ROM memory.

2. A 110, 300, 1200, 2400 baud modem with European and American tones for 110 and 300 baud, auto dial.

3. A card for interfacing an Apple to almost any hard disk. Also needed is a way around the ProDos limit of 2 32-meg disks per slot.

4. A coprocessor/accelerator card that has all three major processors on one card: FAST 6502, Z-80, and 6800 plus 64K ram.

Any takers?

John Nix

(continued on page 22)

AN INTIMATE LOOK AT

(continued from page 5)

Logon unsuccessful—incorrect password. As has just been stated, a valid userid has been entered but the password was incorrect. Passwords can be from 1-8 characters long, but in many cases the minimum length is changed to be at least three characters. There is no difference between upper and lower case letters for either the userid or password as they are converted to upper case by the system. This is another security flaw as it reduces password possiblities.

Password incorrect—reinitiate logon procedure. This is the message received on the older versions of VM/CMS, which means the same thing as the above message.

Maximum password attempts exceeded, try again later. The threshold has been reached for userid and/or password attempts. You will receive this message every time you attempt to logon after exceeding the threshold until a variable period of time (probably from one to five minutes) has elapsed. This locks out *all* users who attempt to login to the system from that particular line. I am not sure whether this is recorded anywhere or whether it is sent to the system console. It's a good idea to determine how many attempts normally trigger this and keep just short of it.

Already logged on. This message will appear when you attempt to logon with a valid userid and password and that userid is already online. Unlike other systems, VM/CMS will not allow the same userid to be logged on more than once.

Userid missing or invalid. As it implies, nothing was typed after entering the LOGON command, or the format for the userid was not correct, i.e. using a number as the first character or a control character used somewhere in the userid field.

Error in CP directory. The CP directory is the main user directory for the system. Entries in the directory contain the userid and password, VM I/O configuration, disk usage values, associated virtual and real addresses, privilege classes, virtual processor size, and other options for each user. Without the proper directory entry, a user cannot logon to the system and will therefore receive this error message.

Command not valid before logon. This occurs when you enter anything other than the commands listed in the menu, i.e. entering BONEHEAD will return this message even though "BONEHEAD" isn't a valid command. Why this is I don't know. So don't get all excited thinking you found a valid command but couldn't execute it since you weren't logged on.

Accounts

By constantly compiling userids from various systems you should be able to collect a nice list of accounts which may enable you to gain access to a system. The following are a few which I have found:

OPERATOR
CMSBATCH
AUTOLOG1
OPERATNS
VMTEST
VMUTIL
MAINT
SMART
VTAM
EREP
RSCS
CMS
SNA

As usual, use the usemame as the password. Things still haven't changed from the Hacking VAX/VMS series...people are just as stupid as they were a few years ago.

There are many default accounts which have the passwords listed in some IBM system manuals. These are hard to obtain and are very powerful since some passwords are rarely changed. If you can get access to the defaults, it will greatly expand your collection of systems—I guarantee it.

Dial

DIAL is used to logically connect lines, whether they be switched (regular dial-up phone lines), leased (dedicated), or logically attached (directly connected), to a previously logged on multiple-access system. The DIAL command is the only substitute for the logon command. On systems running more than one operating system, DIAL is used to connect the user to one of those systems. It is rather common to find two or more operating systems running parallel or "under" one another. This is quite different from most other systems, which run alone on the machine. One machine, one operating system, but not IBM. The ability to have multiple systems running simultaneously and still provide the user with the illusion of it being a single system (the whole idea behind multi-tasking computers is to provide each user with the full resources of the machine so quickly that it appears that he or she is the only one using the system) sets IBM apart from most other computer manufacturers. Some of the systems which run on IBM's are: VM/CMS, MVS/TSO, DOS/VSE, OS/VS1. Some others are: MUSIC, JES, and IX/370 which is IBM's version of UNIX that runs under VM/SP.

It is always good to know what other systems are running, and if you are unable to gain access to the "primary" system, you may be able to gain access to one of the "secondary" systems by use of DIAL. Some systems will require you to specify a line number for certain systems. Others will find a line for you if one is not specified, assuming there are some allocated to that resource. Userids are also dialable. In some cases you have to dial through a particular userid in order to gain access to certain systems or perform certain commands. A typical logon to a DIALed system may look like:

```
.DIAL MUSICB

DIALED TO MUSICB 040

*Miscellaneous Computer Services MUSIC/SP 1.1
SIGN ON.

.RESET

DROP FROM MUSICB 040

VM/370
!
```

When it comes to finding a valid line number for systems that can be reached via DIAL, you could be in for some trouble. If the system requires a line number to be entered (unlike the above example, where line 040 was found automatically), you will not only have to come up with a defined line number, but one that is associated with the system you are attempting to access. Usually you can find this information after logging onto the VM/CMS system in various files, but if you cannot get in, you will have to sequentially enter line numbers. Some that I have seen are 001, 01B, 41A, 040.

The VM/CMS system does not appear to limit the number of DIAL attempts a user can make, unlike LOGON attempts. Programming your micro to search for a valid line number to a system should work with no problem.

To drop the dialed connection just type RESET.

Error Messages

Line(s) not available on 'sysname'. Either there are no lines allocated to the system, or you must enter a correct line number.

Invalid device type 'sysname' 'line#'. You have entered a valid system or userid and line number, but the device you are on (the terminal) is invalid. In this case, a GRAF (Graphics) device, system console, or 3270 terminal may be the only valid device.

'userid' not logged on. The DIAL command cannot be executed unless the user (or system) specified is logged on.

'line#' does not exist. A valid userid/system has been entered but the line number for that userid/system is not valid.

Message

MSG is used to send messages to users who are currently logged on. This command can be issued before (if specified by the logon menu) and after logging in.

```
MSG OPERATOR Help! I lost my password! My userid
        is COMOSOLO.
```

This will send a message to the primary system operator of the system. If there is only one CLASS A user online, the message will be sent to his terminal.

```
MSG *
```

This will send a message to yourself. This is useful for identifying the current userid of an abandoned terminal.

Logoff

The LOGOFF command can be abbreviated as LOG. After logging off you will receive the following:

```
CONNECT= 00:33:54 VIRTCPU= 000:00.28
        TOTCPU= 000:01.76
LOGOFF AT 17:05:44 EST THURSDAY
        04/16/87
```

CONNECT is the actual clock time you spent while on the system. VIRTCPU is the virtual CPU time that was used. TOTCPU is the total CPU time, both virtual and overhead, that was used.

The HOLD command will hold the connection

(continued on next page)

PLAYING WITH IBM'S VM/CMS

(continued from previous page)

allowing you to re-logon again without having to re-dial the system.

```
.LOG HOLD
```

Security Software

There are various weaknesses within VM/CMS both internally and externally which can be exploited. For this reason, various software security packages have been written. There would not be a need for these in most cases if the people in charge of system security knew what they were doing. Anyhow, these packages do provide added security when properly implemented. The most commonly found are VMSECURE and ACF2. TOP SECRET and RACF are others which are less common. These packages are easily identified.

After entering a valid userid VMSECURE responds with:

```
VMXACI1D4R Enter logon password:
***************************
HHHHHHHHHHHHHHHHHHHHHHHHHH
SSSSSSSSSSSSSSSSSSSSSSSSSS
```

One way to positively identify the use of VMSECURE is by using it as a userid. If it is running it will be a valid userid, and who knows, you may even hack the password.

After entering a bad password, ACF2 (Access Control Facility 2) responds with:

```
ACFV1012 PASSWORD NOT MATCHED
ACFV0044 ACF2, ENTER PASSWORD

***************************
HHHHHHHHHHHHHHHHHHHHHHHHHH
SSSSSSSSSSSSSSSSSSSSSSSSSS
```

These packages provide information which *should* be inherent within the operating system itself. Perhaps newer versions of CMS will contain them. Some of these features are:

Last logon date/time
Password expiration
Rules for password selection
Invalidating userids for invalid password attempts
Invalidating terminals for invalid password attempts
Shows users how many invalid password attempts have occurred on their userid
Increased file security

Logged On

After logging on you may receive something similar to the following:

```
OASD 190 LINKED R/O; R/W BY MAINT; R/O BY
        030 USERS
LDGMSG 10:40:25 EST FRIDAY 05/22/87
WELCOME TO MISCELLANEOUS COMPUTER
        SERVICES
VM1
SYSTEM WILL BE DOWN FROM 10:00 TO 10:30
        EST SUNDAY MAY 24, 1987

Logon at 13:22:59 EST FRIDAY 05/22/87
VM/SP REL 4 04/20/86 11:33

R; T=0.01/0.01 13:23:10
.
```

Line #1: This line shows that the disk at virtual address 190 is linked with R/O access by you, R/W by userid MAINT and R/O by another 30 users.

Line #2: This shows that the logon message was created at 10:40 on Friday. Line #3-7: This is the message that is shown to all users of the system upon logging on. Some systems may not have one.

Line #8: The actual time of logon is printed.

Line #9: The current RELEASE of VM/SP and the time and date it was installed is shown.

Line #10: This is the ready message and it is printed after every command is performed where: R=Ready—this indicates that the system is ready for input. T=Time—the first series of numbers tells how long it took the system to perform the last task. The second set of numbers gives the time of day. If you do not receive the ready message you are in CP and must IPL CMS in order to issue CMS commands.

Line #11: The system prompt—you can now enter commands.

Privilege Classes

As with most other operating systems, a user must have sufficient privileges in order to execute certain commands. Every CP command belongs to one of eight IBM defined privilege classes. The CP directory defines which users

(continued on page 20)

2600 marketplace

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.

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

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.

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) 288-6731 and ask for Rick for details.

DO YOU HAVE old outdated computer equipment lying around gathering dust? Why not donate it to 2600's growing bulletin board network? Support freedom of speech in your time! Contact 2600 at (516) 751-2600 or write 2600, PO Box 752, Middle Island, NY 11953.

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 December issue: 12/5.

HACKING INTO IBM'S

(continued from page 18)

can use which classes of commands. Each user has one or more privilege classes, as does each CP command. If you try to issue a command that does not match the assigned privilege class of the userid you are using, the system will not process the command. As far as I know, no records of attempts to use privileged commands are kept.

Here is a rundown of classes A through H.

Primary System Operator: The class A user has the ability to control the system. Any user who uses the VM/SP system console possesses this privilege class. This user can broadcast messages, control system accounting, and issue commands which affect the overall perfomance of the system.

System Resource Operator: The class B user has the ability to control all the "real" resources of the system, except those controlled by the spooling and primary system operators.

System Programmer: Class C users can modify real storage as opposed to virtual storage.

Spooling Operator: The class D user controls spooling data files.

System Analyst: (Class E) Monitors and interprets system perfomance data.

Service Representative: (Class F) This class is usually given to accounts that IBM Field Service personnel use for updates and also for diagnosing system problems.

General User: Class G users are the most prominent on the system. This privilege allows the user to control functions associated with their own virtual machine

Any: The Any classification is given to certain CP commands which are available to any user. The commands are usually limited to Login and Logoff

Class H is reserved for IBM use.

Due to the individual needs of a site, privilege classes can be tailored to suit the facility. A total of up to 32 classes can be made. They would be shown in the CP directory as A-Z and 1-6.

Some typical privilege classes for a few common userids are Class A for OPERATOR, Class F for EREP, Classes B, C, E, G for OPERATNS, and Classes A, B, C, D, E, F, G for MAINT.

Commands

Commands are made up of command names, operands, and options.

Command Name: A command name is an alphanumeric symbol of up to 8 characters.

Operands: These specify the information on which the system operates when it perfoms a command function.

Options: These keywords are used to control the execution of a command. When used, they must be preceded by a left parentheses, but a closing one is not necessary.

Different commands are used within different environments. To see which environment you are in, simply hit retum at the period prompt. You will receive one of the following: CMS, CP, XEDIT.

There are many commands that are useful to both regular system users and hackers. HELP is available on some systems, particularly on university systems. It is extensive but not as clear as UNIX or VMS. This is typical of IBM. Nevertheless, HELP is useful and you should get hardcopies of as many commands as you can. AID is another fom of HELP which may be useful to you in leaming more about the system.

One nice feature of CMS HELP is that when you receive an error message, you can:

```
.HELP DMS000000 or DMK000000
```

Where DMS000000 or DMK000000 is the error message you have received. The system will then explain what it is, why it happened, and how you can correct it.

I am going to hold off on explaining any and all commands related to minidisks until the next section. The others which I have found to be useful are as follows.

You can issue any CP command while in CMS by precluding the command with CP.

Query

Query allows you to obtain various bits of infomation about the system. A full list can be found by using HELP.

One of the most important QUERY commands for the hacker is:

```
.Q NAMES

OPERATOR—01F, SMART—DSC. CMS0349—
B27. LOG00180—B31
VSM—VMVS1
SCOTT—TP11WFM2. CMS1211—TP11WF64,
OPERATNS—TP11WFY1
R; T-0.01/0.01 11:34:28
```

VM/CMS SYSTEM

There can be many users online; usually this list will contain from 30 to 100 users. The last user online was OPERATNS, since it was last in the list. The SMART userid is DSC, or in a disconnected state. Usually a terminal will remain disconnected for 15 to 30 minutes and then is totally logged off the system. If you logon to an already disconnected terminal, the system will reply with "RECONNECTED AT time". The other 2 userids on the same line as SMART are probably connected terminals which are in a pre-logged in or pending logon state. VSM—VMVS1 is another system running parallel to (or under) CMS.

The QUERY NAMES command allows you to gain a little more security for yourself on the system. It allows you to gain more valid usernames to attempt passwords for in the unfortunate event that your current userid dies. Another use is that you can start to compile your "common accounts" list of userids which are found on VM/CMS systems. This list should get larger and larger as you gain access to more and more systems and will allow you to gain access to more systems as it gets larger.

If you can't count how many users are online from the Q NAMES list:

```
.Q USERS
0007 USERS, 0000 DIALED, 0000 NET
```

If you didn't catch the logon message you can view it again by:

```
.Q LOGMSG
```

To see what release of CMS the system is:

```
.Q CMSLEVEL
VM/SP REL. 4, SERVICE LEVEL 417
```

If you are wondering which IBM mainframe CMS is running on, you can issue:

```
.Q CPUID
FF01472343810000
```

This can be interpreted as follows:

```
CPUID= aabbbbbbccccdddd
```

aa= "FF" when running VM/SP. bbbbbb=the processor ID number. cccc=the model number of the system. In the above case, CMS is running on an IBM 4381 system. dddd="0000". This is not used for CP.

SENDFILE allows you to send files within any minidisk that is currently accessed by you to another user. Any time you send a file an entry is made in the file USERID NETLOG (where USERID is the user you are sending the file to). This command is also used for sending NOTE files which can be created with an editor and sent to whomever as E-MAIL.

If you are tired of seeing a text listing, or have attempted to read a compiled program and wish to exit or break out of it, simply hit a hard-break, and then type HX. HX is for Halt eXecution. It will halt whatever you are doing and put you back into the CMS environment. It may take a few lines of text after entering it for the system to stop the process.

This article will be concluded in the December issue of 2600.

(continued from page 10)

interesting users. The number for OSUNY, 2600 Board #1 is 914-725-4060. The Central Office, 2600 Board #2 is reachable at 914-234-3260. If you get a busy signal, just keep trying. Unfortunately, the 914 area code is not yet reachable on PC Pursuit, the service offered by US Sprint that allows unlimited computer time across the country for $25 a month. Let them know you want the 914 area code added—their number is 800-835-3638—so we can all save on phone bills. And keep checking for future 2600 bulletin boards in other areas.

While we're on the subject of bulletin boards, we should point out that the old Private Sector phone number in New Jersey is no longer in use. It's possible we may have sent out some information to new subscribers with that number. If you received such propaganda, please disregard it.

***

In addition to all of this, we now have an address on the infamous "worldnet" discussed in the September 1987 issue of 2600. If you know how to maneuver your way around the networks, you can send mail to us at our Usenet address of 2600@dasys1.UUCP or our Arpanet address of phri!dasys1!2600@nyu. If you have difficulty sending to us at these addresses, let us know.

LETTERS

(continued from page 13)

TAP is Dead!

Dear *2600*:

Can you tell me if a newsletter similar to yours called *TAP* is still being published and if so, what is their address?

D.L.
New York

TAP no longer exists, although back issues are being sold by different people (check the 2600 Marketplace). As far as we know, 2600 is unique in subject matter and approach, although there are some other hacking publications—some good, some bad. Look for reviews in future issues.

In last month's letters column, a reader told us that the 8038 chip used in our 1985 blue box schematic was no longer available. Several readers have notified us to claim otherwise. We understand the chip is obtainable through Janeco Electronics in California (ask any electronics store for their number) at a cost of around $3.95.

listening in

(continued from page 7)

prying ears, probably for reasons of security. The truth is that fed frequencies are as well known as "regular" frequencies. A company called CRB Research, known for publications on surveillance and electronics, has a book called "The 'Top Secret' Registry of U.S. Govemment Radio Frequencies" by Tom Kneitel. This book contains the frequencies, callsigns, and radio codes of every U.S. Govemment Agency in existence, including such agencies as the FBI, CIA, DEA, and of particular interest to phreaks, the Secret Service. Earlier editions of this guide were bound computer hardcopy with everything lumped together and sorted by frequency. This made for something which was difficult to read, and difficult to use. However, it still remained the de-facto scanner guide to the feds, and was very popular.

The recently published (1987) sixth edition has eliminated the readability problems, and has added more non-frequency information which makes for an excellent publication. Inside the 8½ x 11", 192-page book, there is an alphabetical listing of the various agencies. Further delving into the book we find that each agency listing is divided into sections containing frequency/frequency use, transmitter locations/callsigns, and, when available, the various codes and slang used by the particular agency. (Rawhide will arrive at Curbside rather than Pivot.) A particularly interesting section contained the listings for the U.S. Secret Service. Among the frequency/frequency codename/frequency use data was a list containing the codenames used for the presidential staff, first families, and other related information. Did you know that Amy Carter's codename was "Dynamo"?

The Top Secret Registry is an excellent book and is highly recommended reading for those interested in listening to those who are listening to you. It's available for $16.95 from CRB Research, P.O. Box 56, Commack, NY 11725.

And by the way....here are some rather active federal frequencies (in megahertz):

Secret Service:
165.375: "Charlie" nationwide primary channel
166.4625: "X-Ray" common channel for Treasury Dept.

State Department:
409.625

Justice Department:
36.07
411.025

General Services Administration:
(protection of federal buildings)
415.2
417.2

Drug Enforcement Administration:
416.05, 416.325, 418.75, 416.2

CORRECTION:

In last month's list of mass announcement numbers, we neglected to mention that they could also be reached from area code 718.

PHONE NUMBERS OF INTEREST:

212-222-8108	Parents United
718-343-0130	ScrambleFax
800-223-3331	A Bank
011-61-3-692-2982	Recording, wild tone

NOTICE

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind. Simply indicate the amount enclosed and which, if any, back issues you want. Your address label should be on the back of this form.

$15	1 year of 2600
$28	2 years of 2600
$41	3 years of 2600
$40	1 year corporate subscription
$75	2 year corporate subscription
$110	3 year corporate subscription
$25	overseas subscription (1 year only)
$55	overseas corporate subscription (1 year only)
$260	lifetime subscription (never again will we bother you)

Back issues are available. Prices are:

$25	1984, 1985, or 1986 issues (12 per year)
$50	Any two years
$75	All three years (36 issues)

(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

AMOUNT ENCLOSED FOR SUBSCRIPTION: ______

AMOUNT ENCLOSED FOR BACK ISSUES: ______

1984 1985 1986 (circle years ordered)

TOTAL AMOUNT ENCLOSED: ______

(clip and send to us—your address is on the back)

CONTENTS

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