

An Overview of AUTOVON and Silver Boxes

AUTOVON is an acronym for "AUTOMatic VOice Network", and is a single system within DCS (Defense Communications System). It is presently mostly based on electro-mechanical switches, and is a world-wide network for "unsecure" voice communication for the DOD and several related agencies. There is a good deal of basic re-design going on right now, but things don't get changed that fast at the DOD. It works in tandem with AUTODIN (AUTOMatic Digital Network) and AUTOSEVOCOM (AUTOMatic SECure VOice COMMUNICATIONS), and is tied closely to DSCS operation (Defense Satellite Communications System). Just under 200 DCS switching offices around the free world connect about 68,000 government circuits and 73,000 (DOD leased) commercial carrier circuits. Almost all lines in the USA are leased from AT&T, WUI, and GTE.

AUTOVON provides direct interconnect capability to NATO allies and others as well. System service control is entirely hierarchical. Switches respond to 4th column DTMF (1633 Hz mixed with row frequencies—silver box tones—the "missing" row of buttons on your touch tone phone) to provide a means of prioritizing the switching response, where key A is highest and key D lowest priority.

Much work is being done on updating the digital services of DCS to "DDN" (Defense Data Network) but that doesn't affect AUTOVON, it is still all analog. All these systems are basically run by the DCA (Defense Communications Agency) at the

Pentagon. One important office of the DCA is DECCO (Defense Commercial Communications Office) at Scott Air Force Base in Illinois. This office of the DCA manages acquisition and use of all commercial leased lines world-wide. DCA and DECCO also handle lots of other government telecom stuff, like TACNET, the EBS (Emergency Broadcast System), FAA national air system, and reportedly paid some \$1.1 billion for their '84 phone bill all together (15 million miles of leased lines and service). That's at very heavy discounting, too!

How to Participate

You can easily alter your touch tone phone to make it have the extra column that utilizes the 1633 Hz tone. Standard Bell phones have two tone generating coils, each of which can generate four tones. This gives you sixteen possibilities of which you only use twelve. This leaves you with access to the four unexplored tones.

A standard way to modify the touch tone phone is to install a switch to tell it whether to use the silver box tones or not. When the switch is in one position, you will get normal tones, in the other you'll get 1633 Hz tones.

Bell calls these buttons A, B, C, and D, while the army named them, from highest to lowest, Flash Override, Flash, Immediate, and Priority. All other calls are called Routine if no precedence button is pushed. These are used as varying degrees

(continued on page 3-21)

An American Express Phone Story

by Chester Holmes

This story is a memory of hacking a formidable American institution—American Express. No, not AX's internal telecommunications network, but the corporation's toll-free charge card authorization computer. The following can be safely told as our "system" went down a few years ago.

It all started in the summer of 1982. I had been on the lookout for various extenders and other nifty things a phone could link up with. Most were found by scanning and searching 800 number series using the time-honored "hang-up-if-a-human-answers" technique. After a long and fruitless afternoon of such looking, I decided to take a run on down to the local Chinese eatery as my stomach's contents had been depleted several hours earlier. I wasn't wont on dining there; take-out would be fine. Well, as Murphy would predict, my fried rice order wasn't ready at the appointed time, so I found myself at the register with a few moments to kill. Murphy struck again: on the register was a sticker with several 800 numbers and the words "American Express Charge Authorization" emblazoned thereon.

The MSG in Chinese food affects people in a variety of ways. Some folks get rambunctious, but I get sleepy. I told my associate about this number, and told him my right index finger was worn down from hours of dialing. He understood, and made some discoveries while playing with the system all that night.

If I can recall correctly, when one dialed the number (alas, time has erased the number in my brain's RAM), the merchant would be prompted to enter the card number, amount, etc. and the computer would give an approval code. A ## would abort the procedure at any time and disconnect. Merely pressing ## during the call would get an AX operator. This was accomplished by the system obtaining a dial tone and then automatically touch-toning the four-digit extension. We had our fun harassing the operators, for when they hung up, the dial tone would return, but would not automatically dial! We were thus free to make local calls within New York City! We soon tired of this game,

so instead we developed a method of beating the system's demon dialer. Upon dial tone receipt, we quickly touch-toned 9958. The first 9 would give us an outside line, and the 958 was the Automatic Number Identification code for New York. The four system-generated digits would then come through and be ignored. This trick saved us from continual arousal of credit-operator suspicion, and the dial tone was returned after ANI did her thing. We also learned how many different phone numbers they used for this system.

You'll note I said we were free to make local calls. We were able to dial 9-0 to get a Bell operator, who was most happy to assist in placing our long distance calls. For some reason, however, these operators couldn't help with 900 calls (I got the same operator three times in one night while trying to listen to the space shuttle. We developed a kinship by the last call). The AX PBX would give a stern warning if we tried to dial a long distance call directly ("Class of Service Restriction, Class of Service Restriction."), but we soon outsmarted it: it wasn't looking for a 1+NPA etc., but had a timer going, and if you dialed more than eight digits (9+, etc.) in a period of about five seconds, you'd get that message. So we dialed the first few digits, paused, dialed the remainder and the call went through (even to the space shuttle).

Connections were generally less than optimum (in fact they sucked), but if you and your called party were in quiet rooms, you could talk for hours. Another minor annoyance was crosstalk. I had often heard the familiar 9958 off in the background, and once I even faintly heard my buddy. We shouted at one another for a while until one of us hit ##.

I don't think AX was ever quite aware of our exploits on the system since it was on line for several months: a new system was installed when their authorization people moved to Florida. I had had an Amex card all the while, but recently gave it up when they raised their annual "membership" to \$45, and didn't tell me. It was them pissing me off like that that prompted me to tell this tale. I hope you can carry on this tradition, and it's 2600's pleasure to inform technology enthusiasts everywhere of your stories.

final words on VMS

by Lex Luthor and The Legion of Doom/Hackers

(This is the last of our current series on VMS. Please direct any questions to Letters Editor, 2600, PO Box 99, Middle Island, NY 11953-0099.)

Instead of using wildcards for getting a directory listing on the VMS Operating System, try:

```
$ dir [000000...]
Directory SYSSYSDEVICE:[000000]
000000.DIR:1      AMMONS.DIR:1
NEWS.DIR:1       RJE.DIR:1
SECURITY.DIR:1   TEST.DIR:1
Total of 6 files.
Directory SYSSYSDEVICE:[AMMONS]
*INTERRUPT*
$
```

This is a more effective way of listing *all* the directories on the system. The first directory you see will be the directory which lists most every other directory on the system not including subdirectories. The difference between this and DIR [*.*] is that this lists more directories, files than using [*.*]. Usually the directory name is the same as the username thus, even though you have a non-privileged account, you can obtain more usernames to try passwords on. As you noticed, *INTERRUPT* appeared and the dollar sign prompt appeared. This was because of hitting control-y. One neat thing with 4.0 and above is that if you hit a control-c in the middle of a long directory or file listing, it will simply say *CANCEL*, pause for a second, and skip over to the next directory. It will not pause when going on to the next file though. As you know, older versions simply give you the 'S' prompt, so if you wanted to look at something in the 15th directory, you would have to wait for all the directories which are before it, before seeing the contents of the 15th. Now, you can hit control-c and *CANCEL* long directories and sooner, not later, view the desired information. To see more detailed information about the files in your directory:

```
$ DIR FULL
Directory SYSSYSDEVICE:[AMMONS]
INTRO.TXT:5      FILE ID: (929,23,0)
Size:            2/3      Owner:[AMMONS]
Created: 25-MAY-1985 12:38 Revised: 2-MAY-1985 12:38 (2)
Expires: [none specified] Backup: [no backup done]
File organization: Sequential
File attributes: Allocation: 3, Extend: 0,
Global buffer count: 0
- Version limit: 3
Record format: Variable length, maximum 74 bytes
Record attributes: Carriage return carriage control
File protection: System:RWED, Owner:RWED, Group:, World:,
Access Control List None
```

The important information is: the file protection, and if there is an ACL for the file. The FULL qualifier will continue to print the information about each file within the directory.

Devices

On occasion, when you execute a directory search, you will not find much. This is because you are not on the same device as most of the other users are. To change devices:

```
$ SET DEVICE DEVICENAME:
```

Make sure you put the colon after the name. In the case of you not knowing what device to switch to type:

```
$ SHOW DEVICE
```

This will give you a list of devices currently used on the system.

File Extensions

The following file extensions should be used in conjunction with wildcards or [000000...] for viewing all files with that extension: MEM (memo file) These often contain inter-office memos. TYPE this file. JOURNAL (journal file) This is a Journal file, which is created when editing a file. This may contain interesting info. Use TYPE. TMP (temporary file) This is a temporary image of a file. TYPE this file. LIS (list file) Listing file, use same procedure as stated above, i.e.

```
$ TYPE [000000...]*.MEM:*
```

Authorize and the UAF

Earlier, it was mentioned that the file AUTHORIZE.EXE:1 could be found in the [SYSEXEC] directory. It almost always is, but on occasion, you will be able to find it either in the [SYS0.SYSEXEC] or [000000.SYSEXEC] directories. If you are non-privileged, you may wish to see if you can access those directories, and TYPE out the file: SYSUAF.LIS which is a list similar to performing the SHOW * FULL command. When executing that command or viewing that file, the output should look like:

```
Username: SYSTEM      Owner: SYSTEM MANGER
Account: SYSTEM       UIC: [001.004]
CLI:                  DCI:                  I GICMD:
Default Device: SYSSROOT:
Default Directory: [SYSMGR]
Login Flags:
Primary days: Mon Tue Wed Thu Fri
Secondary days: Sat Sun
No hourly restrictions
PRIO: 4
PRCLM: 10
ASTIM: 20
ENQIM: 20
TQIM: 20
MAXJOBS: 0
BYTIM: 20480
PHYTIM: 0
WSDEFAULT: 150
WSQUOTA: 350
WSCTENT: 1024
MAXACCTJOBS: 0
BIOIM: 12
DIOIM: 12
FIIM: 20
SHRFILIM: 0
CPU: no limit
PGFIQUOTA: 200000
```

Privileges:

```
CMKRNL CMEXEC SYSNAM GRPNAM ALLSPOOL DETACH DIAGNOSE
LOG-IO GROUP ACNT PRMCEB
PRMMBX PSWAPM ALTPRI SETPRV TMPMBX WORLD OPER EXQUOTA
NETMBX VOLPRO PHY-IO
BUGCHK PRMGBL SYSGBL MOUNT PENMAP SHMEM SYSPRV SYSCIK
GROUP BYPASS
```

The privileges listed at the end, in abbreviated form, are the important ones as far as security goes:

ACNT: May suppress accounting message.
OPER: Operator privilege.
GROUP: May affect other processes in the same group.
WORLD: May affect other processes in the world.
SHMEM: May create/delete objects in shared memory.
ALTPRI: May set any priority level.
BYPASS: May bypass UIC checking.
SETPRV: May set any privilege bit.
SYSLCK: May lock systemwide resources.
SYSPRV: May access objects via system protection.
VOLPRO: May override volume protection.
READALL: May read anything as the owner.
SECURITY: May perform security functions.

To see what privileges you have type:

```
$ SET PROCESS PRIVS
01-JUN-1985 15:50:56.31 RTA1:User: ACIR508
Process privileges:
LOG-IO May do logical I/O.
PHY-IO May do physical I/O.
TMPMBX May create temporary mailbox.
Process rights identifiers:
INTERACTIVE
REMOTE
$
```

The privileges listed are usually found on low access accounts. If you have the SETPRV privilege, you can give yourself privs by:

```
$ SET PROCESS PRIVS=ALL
```

Security Devices and Software

There are a number of additional security products available for VMS. Some of which are:

Name: ALSP (Applications Level Security Package)

Manufacturer: Integrated Systems Inc.

Location: New Jersey.

Phone: (201) 884-0892.

Cost: \$650.00

Description: ALSP protects system and resource access by restricting users' commands of applications to authorized users. On menu driven applications, ALSP provides further security by checking menu selections against those authorized for a user. Security violations cause LOGOUT and after three unsuccessful access attempts at logon, the user must be reinstated by the system manager. ALSP also generates a message to the system operator when unauthorized users try to access secured data.

Name: DIALBACK and AUDIT

Manufacturer: Clyde Digital Systems Inc.

Location: Provo, Utah

Phone: (800) 832-3238.

Cost: \$980.00 and \$2500.00 respectively.

Description: DIALBACK protects the system by not allowing any dial-in users to make direct contact. It stops them before they can even attempt to log onto the system and requires them to identify themselves. If a user fails to enter a valid DIALBACK ID, DIALBACK will disconnect the line. As soon as DIALBACK recognizes the ID code, it checks a list of authorized users and their phone numbers, hangs up, and calls back the number listed. AUDIT is a sophisticated software security and documentation tool. It allows you to create a complete audit trail of the activities of any terminal on the system.

Name: Data Encryption System (DES) Version II and Menu Authorization Processor System (M-APS) Version I.

Manufacturer: McHugh, Freeman & Associates, Inc.

Location: Elm Grove, WI

Phone: (414) 784-8250.

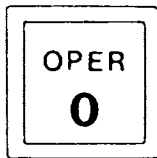
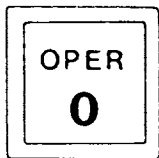
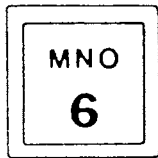
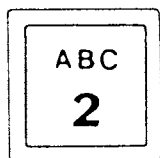
Cost: \$1,250.00 and \$995.00 respectively.

Description: DES runs as a stand alone program (ENCRPT) which allows single or double encryption of system files. DEC encrypts source, data and task image (binary relocatable) files. M-APS provides secured menu access to system applications for authorized users with security displays, and audit trails of movements through the M-APS. Users once captured by the menu cannot escape to the system monitor level.

Conclusion

If all or most security features of VMS were implemented, the system would be one of the most secure around, even more secure than IBM. IBM operating systems such as VM, CMS, MVS, TSO, DOS, CICS, etc. are insecure without the use of additional software security packages such as ACF2, RACF, TOP SECRET, etc. which costs from \$20,000 to \$30,000! DEC didn't do a bad job since the cost of the operating system itself is half that of those packages. But, when computers are concerned, it's the people who are the main factor. Until they realize that hackers can be a real threat, they will continue to leave their systems open to unauthorized access.

(Special thanks goes to The Blue Archer.)



Hacker Zaps Computer Marquee

Phoenix Gazette

A hacker with a perverse sense of humor invaded an Arizona city computer and posted a series of graffiti-type messages on the Mesa Amphitheater's electronic marquee.

Among the notices: "Welcome 2 Mesa: Armpit of the USA" and "Free Phone Sex-(followed by a telephone number)."

The phone number was answered by the wife of Arizona State University President.

One Mesa employee said the amphitheater was "flooded with calls" from citizens after the unauthorized messages began appearing between 9 and 10 pm. The marquee is displayed prominently outside the facility.

The acting director of the amphitheater said he shut down the sign about an hour after the bogus messages began appearing. He said someone using a computer with a telephone modem apparently reprogrammed the sign.

A computer hacker who informed the Gazette of the caper said the marquee program has a "very low security." The hacker, who would not identify himself, said he was not responsible for the sabotage. He said whoever had left the message probably was "just doing a little flexing."

The amphitheater director confirmed that a total of eight messages were displayed, including: "Nancy Reagan Drops Acid," "Support Your Local Clinic," "Hi, Cindy! Let's Party!" "Nuke the USSR," and "Sex, Drugs, and Rock 'n' Roll."

Soviets Denied Computer Access

Combined News Sources

The Defense Department plans to prevent the use of super-computers at American universities by students and Soviet bloc scholars in an effort to minimize leakage of high technology to foreign powers.

The plan, which has drawn sharp criticism from universities planning to install super-computers, is seen by the Defense Department as a protective measure, preventing not only the theft of super-computer technology but also the use of the computers by Soviet bloc nations to solve important technical problems that have direct military applications.

University officials find the Defense Department's attitude ludicrous. They contend that Soviet scholars do not study in the U.S. to steal technology and that closing off university facilities to certain people destroys freedom of academic inquiry.

One university official even said that the plan eventually would turn university faculties into "policemen of advanced technology."

Who Called The Shuttle?

Woodbridge News Tribune

30,000 people called the space shuttle Challenger the day it exploded. The well known "900" number can accommodate up to 7,000 calls at a time. The line was initiated in 1982. 1.2 million calls were placed during the course of NASA missions. AT&T spokesman Rick Brayall claims that it is unknown how many of the callers were actually listening in when the space shuttle exploded 74 seconds after liftoff.

New Ways Of Stealing Data

Administrative Management

It is possible for someone outside a building to read data displayed on the video display tube (VDT) of a terminal or computer. W. Van Eck, a Netherlands Government Agency researcher, said. He said this in a paper he gave at Securicom '85 held in Cannes, France.

Accounts have appeared in the news of the purported use of this technique to compromise word processor displays inside the New Scotland Yard complex. Stories refer to a stunt carried out by members of a BBC-TV news team. Van Eck, in London for an interview after giving the paper, was posed in front of NSY. No reference was made to the identity of the building, and no claim was made that data inside NSY had been compromised.

There have been reports that Polish Government intelligence agents have used this technique to collect sensitive computer data in West Germany. And there have been persistent reports for years that NSA has done such monitoring, involving commercial business sites as well as ones with military intelligence interest.

Van Eck's paper explained that electromagnetic radiation given off by a VDT monitor is unique to that device and is a frequency in the UHF range. It appears that this signal radiates under optimum conditions from 2/3 to 1/4 of a mile from its source, where it can be received and translated into a readable display.

A VDT at the receiving site must be attached to a tunable antenna, an oscilloscope, and other commonly available electronic gear. Van Eck is reported to have checked the material required against a current Radio Shack catalog and found that in their simplest form the necessary components would cost about \$35.

Reportedly, this gear can also be used to monitor messages passing over certain types of cabling that connect computers to modems and printers.

Computer Password Kept Secret

Associated Press

District of Columbia officials who need to use a computer that tracks master financial accounts for the nation's capital are out of luck. No one knows the new computer password.

It was changed by Alvin Frost, a 38-year-old cash management analyst, who says he forgot what it is except that it has something to do with the Declaration of Independence.

Mr. Frost said that he intentionally made the code too complicated to remember so that his superiors in the city's Office of Financial Management would not have access to the system.

He said he changed the code after he found that someone had entered the system and made a copy of a letter he had written to Mayor Marion Barry accusing finance officials of improprieties in the awarding of financial services contracts.

City officials issued Mr. Frost a letter of reprimand after he refused to give the city's assistant treasurer the new password.

Mr. Frost said he did not intend to jog his brain to come up with the password, but added that a thorough reading of the Declaration of Independence would probably remind him.

MAIL WE GET

Dear 2600:

Why are there different subscription rates for "corporations"?

Corporation

Dear Corporation:

Ideally, we are trying to make 2600 available to anyone who wants it. This means that the subscription price must be low. The \$12 individual subscription price barely covers the cost of printing, mailing, layout, and other costs that are involved in producing a monthly publication. One solution is to charge more for those who either have a lot of money; will make lots of copies for their employees; place copies in their library on public display; or stand to gain financially from reading 2600 (those who earn a living beefing up security).

Although we do not copyright our issues, we would prefer that companies refrained from making copies and regularly distributing them. We are told that many do—especially certain telephone companies.

The amount we currently charge for people who represent businesses is rather small compared to many other newsletters and security publications which can actually be in the hundreds of dollars—and many of these are quarterly or bi-monthly.

Finally, for those who have not asked, the corporate subscribers receive the exact same edition of 2600 as do all other subscribers.

Having different subscription rates is a solution that should not hurt anyone. The higher priced subscriptions help us maintain the same service for those who have less money—who are largely the same people who write the articles that appear in 2600.

Dear 2600:

I have call waiting and a modem, so many of my calls are disconnected by the little tone that is sent that tells you someone is waiting on the line.

What can I do?

Dissenting Opinion

Dear Dissenting:

We would like to sympathize, but we don't get nice services like call waiting here.

There are a few ways around it.

*You can disable the call waiting, if you have "selective call-waiting". You dial *70, then get a tone, and from this make your call. Then the call will not be interrupted.*

If you can set the amount of time that the modem can be interrupted for it to disconnect, this may help if you have a smart modem, but the modem at the other end of your phone may hang up anyway.

If you also have call forwarding, you can forward your calls to another line. If you have two lines, you can send the call to your non-data line. If you don't, you can forward your calls to a local test number. Use one that gives an eternal busy signal.

If you are being constantly annoyed by someone who knows he is interrupting, then forward it to a test number that gives silence, a sweep tone, or a payphone somewhere. One way to solve the problem of being annoyed by a persistent interrupter is to call forward to the same number in a different area code where your number would not be valid and it would elicit a disconnect recording. The caller will hear "The number you have reached XXX-XXXX has been disconnected." It's also effective to turn the tables and call forward to another line in the harasser's house, or perhaps one of his relatives. He then winds up harassing himself.

Dear 2600:

Several years ago in upstate New York, I was able to dial 606. hang up and my phone would ring. When I picked up there

would be no one on the line, of course. After some experimenting I found that I could dial 60n, where n was between 1 and 9 and the phone would ring. However, for 601 there was a very short ring and for 609 there was a very long ring and the lengths of the ringing would vary between 1 and 9. What were these numbers all about? Are there similar ways to get your phone to ring now? (Aside from calling up the operator and asking her to call back to test the phone. A fun gag at any friend's house.)

DIAL

Dear DIAL:

It seems that this phenomena is common. You sometimes find it in cross-bar switches. It was probably used to test party-lines.

At our office, you dial 230, then your last four digits and hang up the phone twice, and it will ring back. If you answer it and hang up twice, it will ring back again...ad infinitum. It is not hard to find your ringback if it is only three digits. Just look in your phone book and try out all the exchanges that are not used as standard phone numbers and try them. If you don't find your ring-back, you may find something else interesting, like an exchange that is dedicated to a company or to your phone company.

Dear 2600:

Whatever happened to the famed Bioc Agent 003? Did he go down with Sherwood Forest?

Why not publish all of BIOC-003's files?

Various People

Dear People:

Bioc Agent 003 is alive and well. He has not been whisked off to any penitentiary anywhere, nor has he been scared into going underground as people often have. He is just living his life like anyone else and is doing other things.

Concerning the second question, we do not have the room to print all of his files, for one. Although we have gotten permission in the past to publish some of his writings, we have not looked into the possibility of publishing them all.

Dear 2600:

Do you folks realize that from time to time the phone numbers that you publish have come from my BBS?

Scan Man

Dear Scan Man:

These numbers sometimes come from a BBS, but it is often hard to figure out who found them and finally keyed them in. It is often hard to find out which BBS something may have originated from, because, as you know, good information has a way of spreading around.

We appreciate all you have done for the phreaking industry. (Readers, Scan Man's BBS, Pirate-80 can be found at 304-744-2253.)

Dear 2600:

I have tried calling 8009829999, and I get someone who answers "Operator, what number are you calling?" The audio then cuts out so they cannot hear me. What is this?

A Subscriber in Pa.

Dear Sub:

We tried the number through an operator, and she placed the call but the audio still was cut off. We think what you have here is a special line to reach some telephone company's operators.

Since AT&T has started to cut off the audio on non-supervised (free) numbers, you will sometimes have trouble talking with certain test operators. This has stopped people from using the unsupervised loops that we talked about last fall. These allowed people to call GTD#5 loops for free and meet
(continued on page 3-24)

AUTOVON

(continued from page 3-17)

of priority during wartime and wargame activities. Bell's use of A,B,C, and D is not so clear. However, the last button (D) has an interesting property: on some of the directory assistance lines in the country, it will give you a pulsing dial tone. You can then enter commands to what appears to be a test system for 4A boxes.

How to Use the Silver Box

Call directory assistance using normal tones out of state (NPA-555-1212). Then switch quickly to 1633hz, and press down on the # key (which you've converted to the D key). If you are on an old switchbox (4A), you will get a pulsing dial tone. You will not receive a pulsing tone until the operator actually picks up on the line. If you hear ringing, keep pressing. The tone must be on at the same time the operator gives her "beep". This mainly works with rural information operators.

You can then switch back to normal, and try dialing a 6 and 7. After hearing the pulsing tone and switching to normal tones you can press 6. If another person does the same thing (same area code of course) and presses 7 then you may get a loop-like voice link.

These extra tones are also said to work when using MCI and Sprint and any other long distance services for phreaking. If the service has a six-digit access code then you can simply enter the first three digits and then enter an A tone for the last three digits. This acts as a wildcard tone and eliminates the need to know the last three tones. In this way, one can hack out codes at a thousand per code entered. We'd like to know if anyone has actually done this.

If you have a line on AUTOVON, you call another AUTOVON number by the same process as on the public switched net. To call any DCA office on AUTOVON you dial 22x-xxxx. It breaks down further in hierarchic fashion, so 222-xxxx is DCA directorate, 222-xxxx is also for directors/commanders of major parts of DCA, etc...

Calls into AUTOVON from outside use the area code of the desired AUTOVON location plus public access prefix plus same extension. The exchange gives you the appropriate

AUTOVON switch center, then the local extension (usually last 5 digits) is the same as on AUTOVON. Some examples: the DCA Director is called on AUTOVON by 222-0018, from outside by 202-692-0018. Vice Director is 222-0016 AUTOVON, and 202-692-0016 from outside.

Here are some outside access numbers: 202-692-9012 (DCA Chief of Staff), 202-692-2009 (DCA General Counsel), 202-692-2888 (DCA Chief Engineer), 202-692-6957 (DCA Telecom Regulatory Counsel), 202-692-5358 (Director, DCA Planning and Systems Integration), 202-692-2827 (DCA Comptroller), 202-692-3228 (DCA Commercial Communications Policy Office), 202-692-6007 (Director, DCA Data Systems Support Center), 202-695-2222 (ADP Technical Support Office for above), 202-695-3948 (Computer Services office at above). Under the Defense Communications Systems Organization offices: 202-692-9048 (Director), 202-692-2099 (NCS DCAOC), 202-692-9821 (Plans and Programs office), 202-692-6067 (Satellite Communications System management), 202-692-7475 (Switched Systems manager), 202-692-9009 (Terrestrial Transmission and Systems Control), 202-437-2424 (Defense Communications Engineering Center). Under Command and Control Systems offices: 202-692-8707 (Director), 202-692-5134 (Director, Advanced Development), 202-695-2558 (Information Systems Engineering), 202-695-3118 (National Projects Director), 202-695-1728 (Command Center Engineering), 202-437-2702 (Director, Communications Engineering). DECCO offices: 618-256-4784 (Commander), 618-256-5407 (Office of Acquisition Policy), 618-256-4527 (Comptroller).

The AUTOVON directory is one of the biggest. Calling the 202 NPA and just hacking numbers on AUTOVON exchanges can be both fun and rewarding for the daring! Remember though, a lot of these people can cause you grief if you get serious about harassing or frivolous calls to the same number, so take care!

(Special thanks to Tiger Paws III.)

2600

(ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

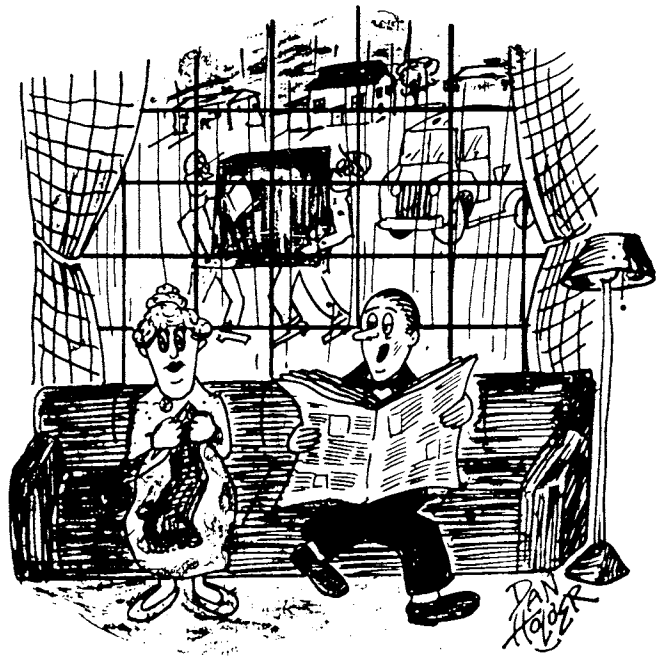
Associate Editors
Eric Corley
David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization
ANNUAL SUBSCRIPTION RATES: \$12, individual; \$30, corporate; \$20, overseas
LIFETIME SUBSCRIPTION: \$260. CORPORATE SPONSORSHIP: \$2600.
BACK ISSUES: \$2 each, individual; \$3 each, corporate; \$2.50 each, overseas
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: 2600, P.O. Box 752, Middle Island, NY 11953-0752
TELEPHONE: (516) 751-2600. BBS: (201) 366-4431
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099
POSTMASTER: This is private mail



"Well, it's either our new television or somebody hacked our Sprint code again."

This month at 2600

It was a lively month at the 2600 office. With the news of **The Private Sector's** return, all kinds of characters were reemerging. We've been getting calls from all over the world about what must now be one of the most famous BBS's in history. Occasionally, we get a call that starts off innocently enough, with someone asking the usual question ("Have you heard anything about The Private Sector?"), and then after we answer them, we realize there are about two dozen other people on the line, representing all different walks of life and nationalities.....We spent a good part of the last month going after two organizations that seem to have betrayed us: **Computel** and **Compuserve**. As mentioned in a letter to us in our February 1986 issue, **Computel** has been advertising their "hacker" publication extensively in many different magazines, most recently in the February issue of *Family Computing*. In spite of all of this advertising, **Computel** has yet to deliver a single issue to anyone that has been in contact with us. We are closing in on them and should have some concrete answers by April. If you've been victimized, gather as much evidence as you can, including advertisements, cancelled checks, correspondence, anything and send it to: Postal Inspector, P.O. Box 2000, Pasadena, CA 91102-2000, Attention: Fraud. We'd like to know how many people were victimized, so please write to us or call.....As far as **Compuserve** goes, we should have listened to many suggestions and never even bothered to get involved with them. But when someone in the office bought a new modem, inside was a neat little package that included some free time on **Compuserve**. OK, free time is always nice, so we figured we'd take a look. We used the temporary id and password supplied with the package, logged in, answered all kinds of questions concerning credit references, etc. before being allowed into the system. By the time we got in, we were so fed up with delays and second-rate appearances that we all took a solemn vow never to call back. And we haven't. A week later, we received our permanent id and password in an unsealed envelope—the post office had even stamped "Received Unsealed" on it. We laughed. We even tried to tell them. They put us on musical hold for over ten minutes and we heard some really good tunes, but then we got bored and decided not to bother. Then one day Emmanuel Goldstein got his Visa bill and

guess what? **Compuserve** was charging us a monthly fee! It seems that the free hour of time you get is not with **Compuserve** but with something called the **Compuserve Executive** system and if you go through the 32-page manual they hand out, you will find on one page in very fine print that there is indeed a monthly minimum for that particular service. Nowhere else do they bother to point this out! Needless to say, we fired off some angry correspondence and we hope once again to see justice served. The last we heard, they had agreed to credit our account for the amount we were charged. Great. We told them to cancel our account. Somewhere in **Compuserveland**, there is a cancelled 2600 account with a credit. We'll keep you updated on these clowns. In the meantime, beware of those "free hour" packets, particularly when the services offering them have a bad reputation.....**Telepub '86** was held in New York on March 8 and was attended by about two dozen people. The future of **TAP**, the old phone phreak newsletter started in the early seventies, was decided. It has none. **Cheshire Catalyst**, its last editor, officially declared **TAP** dead and said that any other magazine calling itself **TAP** shouldn't be taken seriously. We're compelled to agree, but while the time for **TAP** may be done, there are many other magazines that could be started with a little initiative. We hope to hear more on this in the future.....2600 will hold a meeting in New York City. The date and site will be announced in our April issue. Other meetings will be held in the future in other places. Call us if you're interested in organizing one.....We've been getting calls from **England** from phone phreaks there who want loop numbers in the U.S. They want to meet people, they say.....**Postal miracle of the month**: a couple of our staffers were profiled in another magazine. They were described as living in a big, battered house along a wooded coastline in a particular town. No other address for 2600 was given. One day, they received a letter asking about subscriptions with their names on top and "A Big, Battered House Along a Wooded Coastline" plus their town as the only address. Not even a zip code! We were amazed that someone would actually do this and the post office would actually deliver it. We made certain that this request was filled with extra speed. And last week, our letter came back to us: "Return to Sender—Attempted. Not Known."□

2013664431—call it!

The Private Sector BBS is back—and back online.

The bulletin board was seized last July in a fruitless raid by various agents—mainly the government of Middlesex County, New Jersey. Within days the American Civil Liberties Union agreed to defend Tom Blich, the sysop. A cry was heard throughout the phreaking and hacking world, because all those who called the Private Sector knew it never contained any compromising information. After outrageous allegations that mentioned controlling satellites and after six months, the Private Sector was scheduled to be returned on February 16, provided that Blich plead guilty to a token offense. He pleaded guilty to possession of a burglary tool—a small basic program written for Applecat modems.

To date, no evidence of any illegal activity has been traced to Tom, nor has any company or entity ever filed a complaint against him or the Private Sector.

Just a few days before he was to get his computer back, the

Middlesex County authorities told him that they were sorry but they blew up his hard disk controller card. This meant that they could not delete the questionable programs. It also meant that they could not return his equipment.

Finally, someone realized that when a judge says that authorities must give back a computer, they must, so the computer was returned. Tom was told to have the controller card fixed and to send Middlesex County the bill, an uncommon occurrence when it comes to damaged evidence. When he does have it fixed, he's supposed to call up Middlesex and ask someone to come over to his home and delete the questionable files from his hard disk.

With the hard disk temporarily out of commission, the Private Sector is running on two floppies, but the magic is still there. It can be reached at 2013664431 at 300 or 1200 baud. Type NEW to get an account. The software is a little different for the moment; Tom is not sure just how the board will be run. Your suggestions are needed.

SYSTEMATICALLY SPEAKING

Satellite Jammers Jammed

Communications Week

The FCC, perceiving a threat to the operations of domestic satellite systems recently issued a warning that any attempt to jam satellite signals could result in fines as high as \$10,000, prison terms as long as a year, or both.

A few angry owners of backyard earth stations have advocated a form of space vandalism since Home Box Office and others began scrambling the programming they send by satellite to cable TV systems. Publications catering to dish-owners have printed their letters along with other correspondence describing how to jam satellite signals by modifying backyard dishes. FCC Field Operations Bureau engineer Charles Magin said during a press briefing.

"It's a well known fact," Magin said, that satellites are "quite vulnerable" to interference. The vulnerability "is something that the user of the communications satellite has to consider," he said.

About a third of the transponders now in operation are used for video, and most non-video traffic is protected by back-up systems.

"We have means of detecting sources of interference," Magin said, but conceded, "It's very difficult."

[Readers, we would like to know how to jam satellites.]

TASS News Service

Telephone Engineer and Management

The Soviet news agency, TASS, has signed an agreement with the Electronic Publishing Division of Datasolve Ltd. to add its 40,000 word English language news-wire to Datasolve's computerized news service. The service, "World Reporter", is used in over 30 countries around the world.

With TASS, World Reporter will be extending its broad range of authoritative international news and comment from such sources as the Washington Post, Associated Press, Japan's Asahi News Service and the BBC Summary of World Broadcasts, in addition to the financial Times and other major publications.

Soviet Computer Update

2600 News Service H. Alexander

The Soviets are hooking personal computers together with mainframes to collect and process social science documents, according to the Soviet newspaper Pravda.

The USSR Academy of Sciences Institute of Scientific Information in the Social Sciences (INION) and the All Union Scientific Research Institute of Applied Automation of the State Committee for Science and Technology which is connected to foreign East Bloc information banks seems to be running this network. It started during the 1981-85 five year plan. Over 1400 collectives and individual subscribers in various cities can access over 300,000 documents. Data moves through low speed asynchronous modems over telegraph and telephone lines. The plan for the current five year plan calls for INION and the other institute to bring more than 30 large cities of the RSFSR (Russian Republic of USSR) into the network. During this five year plan, the database will grow by 220,000 documents a year. In four years this network might have tens of thousands of users in the USSR and other countries.

Here is a true challenge for American hackers to get into.

V. Vinogradov, academician and a possible head of INION and V. Khisamutdinov, candidate of physico-mathematics,

wrote the article which appeared in Pravda of Dec. 10, 1985. Had this article come out in an American newspaper, it would have told us the name of the service such as NEXIS, the prices, and a number to call to sign up.

[Whenever something becomes important in the USSR, it resolves itself into an acronym. Personal computer now is PEVM which stands for personalnaya elektronaya bychilitel'naya machina. The main network of the USSR Academy of Sciences is know as akademset (academy network), according to the article.]

Dial The Yellow Pages

USA Today

Nynex launched Hello Yello- the first test of operator-assisted Yellow Pages.

Anyone in the test area-- Albany, Schenectady and Troy, New York-- can call 8002222400 toll-free and, for example, tell the operator they're looking for a tanning salon near main street. The operator will search the computer and find the listings that best match your description. You are limited to two numbers per call.

Currently, Nynex is carrying all Yellow Page listings for the test area at no charge, but soon businesses will have to pay to be listed.

[This number can be called from anywhere in New York State.]

Northern To Destroy COs

Communications Week

Northern Telecom is developing a non-public telephone network that will let the manufacturer test and break equipment before introducing the gear for public use.

The \$40 million "captive" network goes on line in late March and will eventually let Northern Telecom push central-office and remote systems to a test capacity of 600,000 calls-per-hour.

"We'll be able to test to destruction," said company spokesman Tom Hill. "We can put a piece of hardware in there and overload it and overload it until it breaks. Then we'll take it apart and figure out why it broke."

The company said a primary use for the captive network will be experiments, conducted in conjunction with Northern Telecom's telco customers, to test Integrated Services Digital Network (ISDN) applications.

Northern calls the laboratory network FAST for First Application System Testing. FAST will be equipped with a DMS-100 200 central office switching system and peripheral equipment.

It will be able to simulate most of the hardware and software configurations and traffic loads encountered in actual network use.

There Are More Phones Than Ever

Associated Press

Despite rising costs for basic telephone service, more households than ever before have a phone, the FCC announced.

The 91.9 percent figure is the highest ever recorded. Another 2 percent have a phone available in a hallway or somewhere nearby where the family can receive a call.

There is a phone in 97.1 percent of the houses and apartments in Connecticut-- highest in the nation-- and 81 percent of the units in Mississippi-- the lowest.



2600 WANTS YOU!

Join the staff of 2600. It is simple. Just compile any information you have so it is easily understandable and send it to us. We accept hardcopy and uploads. We will also accept information on floppies—call us if you wish to do that.

We need:

- Profiles of long distance companies
- Profiles of computer systems
- Reviews of popular security devices
- Lists of interesting phone numbers
- Lists of interesting reference books and magazines
- Updated tutorials on using things like ADS, CNA
- Interesting true stories
- Data that can be a good reference
- Maps of computer networks
- Analysis of new legislation

We would like:

- Legitimate access to various computer networks
- You to continue to send your comments and questions
- You to continue to send clippings from local papers and magazines
- You to keep us informed

Things we could always use:

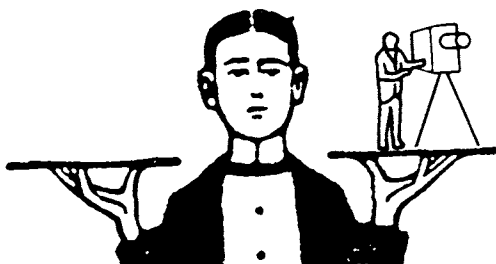
- ★ S-100 Bus equipment
- ★ A hard drive
- ★ Printers, computers, telephones, and interesting devices
- ★ A copy machine
- ★ A newer, voice activated answering machine
- ★ A 2400 baud modem

If you send an article or data, please request a by-line otherwise we will not print one.

If you send us hardware, please make sure it is not stolen. We do not want your troubles.

We now have bright red Day Glow stickers for your local payphones. If you want to help distribute them, contact us! Finally, if you are at a college, please let us know, and we will send you a publicity kit, so you can help us reach college students on your campus. Please tell us about your college (how big it is, specialties, etc.) If we get a new subscription from your campus, the first \$12 goes to you!

All contributors, please send your gifts to: 2600, P.O. Box 99, Middle Island, NY 11953-0099, or call 5167512600.



LETTERS

(continued from page 3-20)

each other from anywhere in the world.

It is possible that this 800 number is one of those numbers where the audio cuts off as a result of AT&T's handiwork.

If you call 6124251999, which we are told is unsupervised, an operator will answer. If you remain quiet, then she is likely to put a recording on the line that explains how you may have trouble talking with special operators.

Dear Readers:

In last month's story titled "It could happen to you", the inevitable happened. We mixed Person A up with Person B and in the last two paragraphs their roles were reversed. We're terribly sorry about this and we're optimistic about the chances of it never happening again.

Recently, perhaps as a result of that story, we have heard that A might be getting his phone back and that New York Telephone security may actually start believing A's story—especially after the error message on A's old line was changed by someone to say calls are being taken at the home phone number of the head of telco security!

We will keep you informed on this one.

YOU CAN HAVE THIS SPACE TO ADVERTISE YOUR BBS!

Send \$5 your BBS name, number, and any information about it to: 2600 BBS Classified Dept - P O Box 762 Middle Island NY 11953-0762 Send only BBS classifieds, please

By Hackers For Hackers

- ELITE BOARD DOWNLOADS
- CRACKING TIPS
- PHREAKING SECTION
- GAME CHEATS
- PARMS
- PROGRAMS
- INTERVIEWS
- ADVENTURE TRIPS
- HACKING TIPS
- MYSTERY SECTIONS

Published on both sides of an Apple diskette - 4 times a year.

The BOOT-LEGGER MAGAZINE

Subscribe Now!

Send 25 Bucks for a 1-Year Subscription
THE BOOT LEGGER, 1080 Hays Road,
Cave Junction, Oregon 97523.
Overseas Subscriptions \$50.
Canadian \$30 U.S. Currency.

FOR AD INFO. & QUESTIONS
CALL BOOTLEG AT (503) 592-4461

EQUIPMENT

Security, Privacy, Police
Surveillance, Countermeasures, Telephone

BOOKS

Plans, Secret Reports, Forbidden Knowledge

SEND \$20.00 FOR LARGE CATALOG AND ONE YEAR UPDATES

SHERWOOD COMMUNICATIONS

Philmont Commons
2789 Philmont Avenue Suite #108T
Huntingdon Valley, PA 19006