vms—the series continues

by Lex Luthor and The Legion of Doom/Hackers

The VMS Operating System supports all VAX-11 series computers. The system permits an absolute limit of 8192 concurrent processes. This depends on the physical memory and secondary storage available. The practical limit is in excess of 100 concurrent users for a large scale system. The initial license fee is $10,000, and when run on the VAX 8600 the fee is $15,000. There are an estimated 22,000 sites running VAX/VMS. UNIX is the operating system which can run on both the VAX and PDP machines. In this series we will explain in detail the more useful commands, notable differences of Version 4.0 and higher, and the new security features and software available for VMS.

Logging In

```
Username: NCR508LOD
Password:
LOD/H Network Communications Resources
VAX/VMS Version 4.2
Last interactive login on Wednesday, 01-JUN-1985 10:20.11
Last noninteractive login on Friday, 30-MAY-1985 15:38.27
2 failures since last successful login
You have 1 new mail message
$
```

All login procedures are executed by one of two methods, interactive or noninteractive. Interactive logins require the user to follow the prompts of the system for information. Noninteractive logins are performed exclusively by the system without user interaction.

Types of logins are: 1) Local: This is executed by a user who is directly connected to the CPU; 2) Dial-up: Login using dial-up lines; 3) Remote: Remote logins are performed to a node over a network; 4) Network: Network logins are noninteractive as they are accomplished automatically when a user accesses files stored in a directory on another node or performs a network task on a remote node assuming they are both nodes on the same network; 5) Batch: A Batch login is another noninteractive automatic procedure performed when a batch process initiated by a user actually runs; 6) Subprocess: Subprocess logins are always noninteractive although it is also a result of a user executing either a specific process form of a command or a system service. Other types are: Proxy login, a type of network login permitting a user to access files across a network, or a Detached process login which can be specified by the user as either interactive or noninteractive. It is a result of a user executing either a specific process form of a command or a system service.

Common Accounts

Here are some more common accounts which may enable access. One note—there is a difference between default and common accounts. Defaults are put in by the manufacturer, and common accounts are characteristic of most computers or operating systems of the same make.

Username:	Password:
RJE	RJE
HOST	HOST
LINK	LINK
INFO	INFO
BACKUP	BACKUP
NETWORK	NETWORK
DECMAIL	DECMAIL
HELPDESK	HELPDESK
REPORT(S)	REPORT(S)

As you have noticed, we are relying on the user to use their username as a password. If none of these work, first names, social security numbers, initials, etc. might work.

Password Security

Passwords can be selected by the user or automatically generated by the system. User selected passwords require a minimum length of characters to prevent use of familiar easy-to-guess words. Automatically generated passwords offer the user a choice of randomly sequenced characters resembling English. All passwords need to be changed about every 30 days and are one-way encrypted when stored. There are 2 levels of passwords used. A user password is required of the majority of users. A system password is required prior to a user password when restricting access to a particular terminal. For maximum security two user passwords may be required, a primary password and successively a secondary password. I have not encountered this yet, but I thought I would just mention the capabilities of the VMS security system.

Interior Barriers

On some systems, after successfully logging on with the username/password combination, the system may ask you to enter a dial-up, modem, remote, etc. password. It may dump you into an application program or it may give you a device not found error. In any case, this prevents you from gaining access to the operating system. A possible way around this is to hang up and call back the system, hit control-c and/or control-y after the initial logon sequence. This will prevent the system from executing the security program, login.com file, application program, or detect that there is not a device assigned to the user in question. This might have to be tried a few times, since timing may be crucial. Most likely, it will not be possible to break out of the program itself after logon,

because of the command "set nocontrol=y" which inhibits the use of control-y. If this doesn't work, then set nocontrol=y has been implemented from the start of logging in, which is accomplished by running authorize and changing the user characteristics in the UAF. But this is usually not done, whether it's because the system manager is lazy, ignorant, or maybe the use of the control character is needed later in the logon session. Thus, unauthorized access to the machine is often gained.

Security Features

Security for VMS is based on the reference monitor concept. Under this concept the reference monitor is the central security point for the following: 1) Subjects: users, processes, batch jobs; 2) Objects: files, programs, terminals, tapes, disks, mailboxes; 3) Reference monitor database: user authorization files, rights database, file protection, access control lists; 4) Security audit. The reference monitor system mediates every attempt by a subject to gain access to an object. The greatest advantage of VMS is its flexibility. The system manager can choose to implement or ignore a wide range of security features. Fortunately for the hacker, they all seem to ignore the important ones. It is possible to protect all, any, or none of the files created. It is also possible to provide general or restricted passwords, or no passwords at all. Access codes can be global or limited. The use log can be ignored, used only for record keeping, or be employed as a security control tool. Finally, the encryption system can be activated where needed, defaulting to uncoded material for normal use.

VAX/VMS has the following security features that are designed to prevent unauthorized access or tampering: 1) Provides a system of password controls and access levels that allow the security manager to open sections of the system only to those users with a particular requirement or legitimate interest; 2) Keeps a careful log of all interactions so that questionable uses can be challenged and documented; 3) Supports an encryption system that allows system management to create coding keys that are necessary for access to programs or databases. The encryption system of VAX/VMS provides an additional level of security, however the other security features are sufficient to deter most losers. The encryption system included in the operating system package would probably not stop those few so motivated. The encrypt facility does not use a sufficiently complex algorithm to be unbreakable, although it would slow down or halt most potential abusers.

Internal Security

VAX/VMS determines access to objects by utilizing two protection mechanisms: Access Control Lists (ACLs), and User Identification Codes (UICs). It takes the two together, acting with user privileges, for access.

Access Control Lists: The ACL uses identifiers to specify users. There are three types: 1) UIC identifiers depend on the user identification code that uniquely identifies each user on the system; 2) General identifiers are defined by the security manager in the system rights database to identify groups of users on the system; 3) System-defined identifiers describe certain types of users based on their use of the system. An ACL consists of one or more Action Control List Entries (ACEs). There are three types of these: 1) Identifier ACE: This controls the type of access allowed to a particular user or group of users. Access types are: READ, WRITE, EXECUTE, DELETE, CONTROL, and NONE; 2) Default protection ACE: This defines the default protection for directory files only; 3) Security alarm ACE: Watch out for this one! It provides an alarm message when an object is accessed. This will alert managers to possible security threats. Alarms may be generated when an unauthorized user performs the following access types: READ, WRITE, EXECUTE, DELETE, or CONTROL. Alarms are also issued for the SUCCESS or FAILURE of these attempts.

User Identification Codes: As stated in an earlier installment, each user has a UIC. Each system object also has an associated UIC, defined to be the UIC of its owner, and a protection code that defines who is allowed what type of access. Also mentioned earlier was the protection put on objects: System, Owner, Group, and World. Depending on these, the protection code can grant or deny access to allow a user to read, write, execute, or delete an object. When you log in, the identifiers which are in your "rights database" are copied into a rights list that is part of your process. The rights list is the structure that VMS uses to perform all protection checks.

Audit Trail

The security log feature, if monitored, and that's a big if, is a major disadvantage for the hacker. Flag codes can alert an operator to an ongoing hack; review can isolate users attempting to exceed access restrictions. The system can "freeze" a terminal if a breach is discovered, or if multiple wrong access codes are attempted. Of course, the log system functions somewhat after the fact and it is possible, though difficult, to alter the security log. A terminal can be designated as an audit alarm console and all auditable events are displayed on the console. Some events, such as certain login failures and uses of privilege are always auditable. Other events, such as successful or unsuccessful attempts to gain access to sensitive files, can be selected by users or security managers for auditing. For example, the owner of a sensitive file might create an ACL entry requesting that all accesses to that file be audited. Whether someone reviews that audit is another story.

It Could Happen To You!

A bizarre story is unfolding in New York City, one which typifies both hacker ingenuity and corporate indifference to the average customer.

It all started when Hacker A met Hacker B on a loop somewhere. At first they got along quite well, exchanging all kinds of information. Over time, however, Hacker B got more and more obsessed, while Hacker A wanted to get on with a normal life. B would not stop calling A, which led A to tell B that if he didn't stop bothering him, he would get the authorities on his case. Well, B didn't and A did. And that's where the trouble really started.

For the last couple of years, almost every few minutes, A's phone has been ringing. At the other end is either B or someone or something that B has programmed. Sometimes nothing is said; sometimes a threat is uttered; sometimes the caller just laughs. A and his family have been trying, literally for years, to put an end to this. At first they simply changed the number to an unlisted one. Within an hour, B had found the new one. So they tried to change it again. New York Telephone refused. Either they would have to pay an exorbitant fee this time, or the number would not be changed. They said it was impossible for somebody to find out their number so fast—he must have been told by somebody in the family.

This scene was repeated a number of times, with A's family changing their number practically a dozen times and having to pay the fee for most of them. It reached the point where B would call them *before* they received their new number to tell them what the new number would be.

This wasn't all. B had also managed to charge outrageous amounts to the family's phone bill. He would call their answering machine collect on a long distance trunk and make it sound to the operator as if someone had said "yes". Then he'd leave the connection open for hours. He also managed to place third party calls, using their number as the billing number. Their bill was outrageous and the phone company insisted that they were responsible for it. Their service was disconnected when they didn't pay and today they are slowly paying back the huge debt.

Meanwhile B has tried to get the authorities to look at A (whose address and phone number he has), with only lukewarm interest. The FBI says it has an eye on him, but won't help B deal with the phone company.

To this day it continues. The calls keep coming and B is powerless to do anything. A knows the phone system like the back of his hand and he can make it do almost anything. The phone company does not want to admit this and, on many levels, is incapable of understanding it themselves. The result: an innocent victim gets it from both ends.

DIAL BACK SECURITY

A computer security device that is often referred to as being foolproof is the dial back system. In the case of a dial back system, a computer has a dial up access number where users may enter their user IDs and then their passwords. Then they hang up or are disconnected from the computer and the very system they just called will call back on a prearranged number after a short period of time. The hacker cannot penetrate this because after he discovers the working ID/password combination, he cannot do anything but hang up and wait for the computer to call out to the prearranged number. It is extremely difficult for a hacker to receive a call at that prearranged number, unless he taps into the cable-pair at the home or office of the person who owns the account and then uses a portable computer and modem while squatting in a sewer, on a telephone pole, or perhaps in bushes.

The number itself is not specified when the call is initiated, but at some previous time, usually when the account was first set up. Many companies rely on dial-back systems for protection and will walk around smiling, lost in nirvana over how secure their systems are—how foolproof they are. But these systems are potentially vulnerable. These vulnerabilities are due to the phone system and the modems used, and make it all too possible for a hacker to connect to the callback call and fool the modem into thinking it had dialed the legitimate user.

How

Some older telephone switches use caller control where the call is only disconnected if the caller who originates the call hangs up. This means that a modem could not hang up on a caller—usually a local caller—who dialed into the computer. The modem would go "on hook", and the computer would think that it hung up, but the caller would still be there the second it picked up again to make an outgoing call.

The modem might not notice that they were still there and would attempt to dial and then wait until the call went through and for a modem to pick up. After a short period of time an answer tone could be sent, and they would be connected to the system simply by not hanging up.

Of course, some modems incorporate dial tone detection before dialing and ringback detectors. These will not dial until they "hear" a dial tone and then a ring, but these could be fooled with a recording of a dial tone or a ring.

Some modems will even try to pick up a ringing line and attempt to make an outgoing call on it. This could be used by a system penetrator to break dial back security even on joint control or called party control switches. A penetrator would merely have to dial in on the dial-out line, just as the modem was about to dial out. The same technique of waiting for dialing to complete and then supplying an answerback could be used as well as the recorded dialtone technique.

Calling the dial-out line would work well in cases where the modem has disabled auto-answer because it was about to pick up (answer) the phone in order to start dialing.

Even carefully written software can be fooled by the ring window problem. Many COs actually will connect an incoming call to a line if the line goes off hook just as the call comes in without first having put the 20 Hz. ringing voltage on the line to make it ring. The ring voltage in many telephone central offices is supplied asynchronously every 6 seconds to every line on which there is an incoming call that has not been answered, so an incoming can be answered in some cases before a ring can be detected.

This means that a modem that picks up the line to dial out just as our penetrator dials in may not see any ring voltage and may therefore have no way of knowing that it is connected to an incoming call. And even if the switch always rings before connecting an incoming call, most modems have a window just as they are going off hook to originate a call when they will ignore transients (such as ringing voltage) on the assumption that they originate from the going-off-hook process.

It is impossible to say with any certainty that when a modem goes off hook and tries to dial out on a line which can accept incoming calls it really is connected to the switch and actually making an outgoing call. And because it is relatively easy for a system penetrator to fool the tone detecting circuitry in a
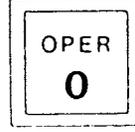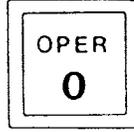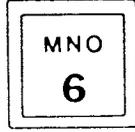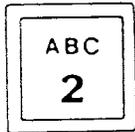
Teenagers "Abuse" Party Line

Associated Press

Northwestern Bell has cancelled a teenage-oriented telephone chatting service, which some callers used to solicit sex and arrange drug deals. The service, known as GABTEEN, had been in use for two and a half months. It was discontinued less than 24 hours after reporters from WCCO-TV in Minneapolis gave them transcripts of conversations they had tape-recorded.

"What they showed us were transcripts of conversations regarding explicit sex, extreme profanity, and conversations dealing with drugs and drug purchasing," company spokesman John Walker said.

"We had anticipated there would be some profanity, and we fully expected there would be some language that would be unacceptable to some people," he said. "But clearly, what WCCO outlined calls for much closer scrutiny as to the way we present this service in the public marketplace."

A Unique Obscene Caller

Newark Star Ledger

A Montville (NJ) High School music teacher has been charged as the man who made hundreds and perhaps thousands of obscene telephone calls to area women while impersonating a police officer during the past two years, Morris Township police have announced.

According to police, the suspect is accused of making random calls to an undetermined number of women posing as an "Officer Brill," who claimed he was investigating harassing and lewd calls.

"He would seek the women's cooperation, asking them to go along with anyone who placed an obscene call to them," a detective said. "Then he'd call the person back and engage in a conversation filled with vile and lewd language. In some cases, he would even contact the woman again, asking her to repeat the language used in the call. The calls were made for some type of sexual gratification."

Authorities were frustrated until late November when a case was opened concerning a woman being subjected to harassing calls. A "trap" was placed on her telephone line, allowing the calls to be traced. The suspect made a random call to this woman and New Jersey Bell was able to trace it to him. An investigation of the defendant was then begun that included a stakeout of his residence and the placement of a court-authorized device on his phone line that prints out all numbers called from that location [known as a pen register].

Police said the subject would "fire off" as many as two or three calls a minute until he encountered a woman's voice that appealed to him.

The Scoop on Pen Registers

The New York Times

A Congressional survey has found data indicating that Federal law enforcement agencies (such as the FBI and the IRS) installed secret electronic devices to record telephone numbers that were dialed from 3,400 telephones in a recent 12-month period.

Unlike telephone taps and room bugs, which record actual conversations, these devices are not covered by the Federal and state laws restricting electronic surveillance, and the Supreme Court has ruled their use does not violate the Constitution's provision against improper Government searches.

Federal and state wiretapping laws generally require the police to obtain a special warrant before installing the more prying surveillance devices and to make annual public reports summarizing the total number of interceptions for each tap, the number of people who have been overheard talking, and the number of people indicted. For instance, in the 1984 calendar year, Federal agents obtained warrants for 289 taps and bugs that were operated from one to 360 days. As a result, 50,147 persons were overheard making 576,775 conversations. This resulted in 795 arrests.

In the last few years the Supreme Court has handed down several decisions holding that the information collected by the simpler number-recording devices does not require any legal protection, largely because the court concluded that which numbers were dialed from a telephone was far less revealing than actual conversations. However, officials of such organizations such as the American Civil Liberties Union and AT&T [surprised?] have contended that a record of what numbers a person dials, the length of each conversation, and the times they were made can provide a revealing portrait of who someone's friends and associates are and what are the target's daily habits.

These number-recording devices were used even before the computer era; they kept track of the number of clicks as a dial spun back into place. A pen would make a mark for each click, which accounts for the name "pen register".

Reporters Steal Swiss Phones

Combined News Sources

Reporters covering the US-Soviet summit in Geneva boosted the profits of the Swiss telephone company by spending about $1 million to file their stories. The money spent on telephones and telex messages will mean a net profit of $500,000 for the state-owned postal and telecommunications service, said Oscar Gada, customer relations director.

But the profits will be reduced by the money it will take to replace the telephones that disappeared. "We are up to 50 missing phones so far and are still counting," Gada said. "They probably were kept as souvenirs."

The 3,000 reporters made 10,000 phone calls, 1,600 of them collect, and there were 937 telex calls representing 1,631 full pages or 190 hours of transmission time.

Gada said the agency did not receive a single complaint about its summit service and even received a letter of thanks and congratulations from US Secretary of State George P. Shultz.

Pay Phone Causes Panic

Combined News Sources

A ticking sound from a telephone sent 50 travelers scurrying behind ticket counters at the Monroe (Louisiana) Regional Airport to shield themselves from what they thought was a bomb.

But the ticking just meant that the telephone's coin box was full of quarters, nickles, and dimes, police said.

Monroe police, airport security officers, and the Monroe bomb squad approached the phone cautiously, in case a bomb had been planted inside.

A slightly embarrassed police spokesman said it was the "totalizer," a mechanism that clicks when the coin box in a pay phone has been filled up.

Dear 2600:

My high school has a PDP with 48 VT101 terminals. They are very reluctant (probably just ignorant) to give out any sort of information. They feel that the system's use is only for learning Basic and Pascal—no experimentation. But this should be expected.

I have inquired many times about controlling the cursor and the graphics on VT101 terminals, and they have threatened and warned me not to play with things I don't know. I am requesting information on where I can acquire information on the VT101 terminal (books, companies, etc.). If you could publish this information I am positive many readers would find it useful.

Artful Dodger

Dear Dodger:

Perhaps one of our erudite readers will send us such a list.

In any case, yours is a familiar problem—one that breeds the hacker instinct.

Dear 2600:

Here are some notes on the schematics you published in your October, 1985 issue for a "blue box".

A) The power supply that regulates the 18V input to 10V output is not necessary. While the dual battery arrangement will provide longer operating time between battery changes, it is possible to operate this device with a 1.9V battery. I would, however, recommend the use of 'high power' alkaline batteries.

B) The variable resistor that controls the tuning of the 1500 Hz tone is omitted from the schematic. It should be on the wire between the 1300 and 2600 resistor locations.

C) The 8038 chip, made by Intersil, is no longer carried by many Radio Shacks. I understand that stores will not be restocking this chip after their current stock is depleted. I would recommend that people acquire this chip from Advanced Computer Products Inc. (8008548230) at a cost of $3.75 each.

D) The 20K, 15 turn resistor is sold by Radio Shack at $1.49 apiece (PN 271-340). I suggest that these parts be bought through mail order houses (such as Digi-Key (800DIGIKEY)) at an approximate cost of $1.20 apiece, or 10 for $10.

E) Items (c) and (d) allow the hardware oriented person to construct this frequency generator for under $30.00 if most or all parts are bought through non-retail houses.

F) It is possible to make a very 'professional' generator by replacing the switches with the keyboard from an old or discarded calculator. They will require extensive modification though (as the generator cannot directly utilize a matrix keypad). The basic idea is to peel off the plastic covering and cut traces and add jumpers so that each key becomes a totally separate switch. Texas Instruments calculators have a keypad that isn't too hard to modify this way. If you use this type of switching, you'll find that the single largest component will be the speaker, and the battery running a close second.

Field Support

Dear Readers:

We have an update to last month's letter from The Creature who discussed using a port selector in the terminal room at the University of Southern California to gain entry to an IBM mainframe.

Recently the University upgraded the port selector device. It no longer recognizes abbreviations for system names. Also, it has been upgraded so that you can't randomly connect to other people's jobs.

Another update: we have been told by at least three callers that there is a mistake in last month's Basic program for the Commodore 64. On line 170 the "U" should be a "T", and on line 175 the "T" should be a "U". One of the callers said that the program did not work anyway. He said that "only one tone

would break the dial-tone." Note: this program produces MF tones and not touch tones. We have indicated in past issues how they can be used. We hope that the programs worked for you.

If you have other programs, plans for electronic toys, as well as profiles of your favorite extenders or computer systems, or even useful data, be sure to send them along to us.

Dear 2600:

Your December issue containing the BBS numbers arrived in mid-month. I called all the numbers in my area code and got a computer on only two out of fourteen numbers. One of those is Bonneville Communication's Teletext 5 (part of our local TV station). The rest are private lines, some to dial phones. I would appreciate more information next time as to ring-back or whatever answering system is in use.

Fellow in Utah

Dear 2600:

We subscribed to *Computel* more than a year ago. To date, we have not received a single *Computel* issue. You commented about *Computel* in your issue 2-15. Several times, we complained to *Computel*. And several times we were contacted by Mr. John Reynolds, each time with a dumb excuse and assurance that the issues were forthcoming. We weren't the only ones stung by *Computel*. At least a dozen of our readers informed us of similar experiences with *Computel*. I am convinced that *Computel* was/is an FBI sting operation. Consider:

1) *Computel* advertised for more than a year in most issues of Computers and Electronics, Radio Electronics, BYTE, and other computer magazines. We ran a rough survey of their advertising and came to the conclusion that *Computel* spent close to $100,000 on advertising alone!! For most of this period, *Computel* also had a toll-free number.

2) During this entire time, *Computel* never produced a single issue that we know of! At least five of our readers stated to me that they complained to the Postal Inspector and to the magazines about *Computel's* lack of fulfillment. None of these five people received any kind of response from the Postal Service or the magazines, and *Computel's* ad still persisted many months later! In the decade-plus that we've been in the mail order business, we have seen a lot of mail order firms lose their advertising within three months of the onset of non-fulfillment complaints to the magazines.

The size of *Computel's* operation and the apparent flaunting of the law with impunity very strongly implies that *Computel* was part of a government scam. We suspect that this scam was conducted for two reasons:

1) To compile lists of folks involved in and interested in phreaking of all types.

2) To purposely rip off folks interested in phreaking to discourage them from subscribing to future legitimate phreaking publications. To damage publications such as those produced by Consumertronics Co., *2600*, and other technological anti-establishment publications.

John J. Williams, Consumertronics Co.

Dear Readers:

We hope this was not true, but we also got complaints from people who received nothing more than promotional material. We did not receive even that much.

Over the last year, we called the offices of Computel several times and got the same types of responses that Mr. Williams got.

We hope that our readers can investigate this matter on their own, or perhaps even visit Computel's office in Van Nuys, California. They can be reached toll free over Skyline by calling 950-1088 and entering "2COMPUTEL" after the tone.

Number	Description
011-44-1-246-8000	STARLINE
011-44-1-246-8017	DIALING INSTRUCTIONS
011-44-1-246-8020	TELECOM SPORTS REPORT
011-44-1-246-8030	TELECOM TRAVEL LINE
011-44-1-246-8031	TELECOM TRAVEL LINE
011-44-1-246-8032	TELECOM TRAVEL LINE
011-44-1-246-8033	TELECOM TRAVEL LINE
011-44-1-246-8035	LONDON RADIO
011-44-1-246-8060	TELECOM RACING BULTN
011-44-1-246-8088	CIVIL EMERGENCIES
011-44-1-930-4832	QUEEN ELIZABETH
011-44-61-165000	TV SCHEDULE
011-44-61-166000	STOCK REPORT
201-623-0150	Stock Quotes
201-686-2425	UNION OIL
202-224-3081	Joint Economic Comm
202-224-8541	Senate Floor Activity (Dem)
202-224-8601	Senate Floor Activity (Rep)
202-225-1600	Dem Legislative PGM
202-225-2020	Rep Legislative PGM
202-225-7099	Botanic Garden Events
202-225-7400	House Floor Activity Dem
202-225-7430	House Floor Activity Rep
202-252-4333	Jobsline-Dept of Energy
202-270-9000	Christian Message Line
202-275-2183	Jobsline-Govt Printing Off
202-275-6361	Jobsline-General Accounting
202-287-4091	Treasury Dept-Securities
202-287-4100	Treasury Dept Auction Dates
202-343-1100	EPA
202-343-2154	Jobsline-Dept of Interior
202-343-3020	Newsline Dept of Interior
202-347-3222	F.A.A.
202-357-2000	Dial-A-Phenomonon
202-357-2020	Dial-A-Museum (Smithsonian)
202-357-8555	Energy Reg Comm
202-393-1847	Ec Highlights Dept Of Comrc
202-393-4100	Economic News
202-393-4102	Weekend Preview Dept/Comrce
202-426-1921	Newsline-Dept Trans
202-426-6975	Natl Parks Info DC Area
202-447-2108	Jobsline-Dept of Agr.
202-447-8233	Natl Grain Summery
202-456-1414	White House
202-456-2100	Presidential Press Office
202-456-2343	President's Daily Schedule
202-456-2352	CIA Intellegence Switchbd
202-456-6269	First Lady's Daily Schedule
202-472-2729	Newsline-Dept of Education
202-488-8358	Events & Highlight
202-523-3540	Newsline-Fed Trade Comm.
202-523-5022	Newsline- Govt Policy Wash
202-523-6899	Pressline-Dept Labor
202-545-6700	PENTAGON
202-545-6706	Pentagon
202-632-0002	FCC Newsline
202-632-0580	Jobsline-Dept. of State
202-633-3121	Jobsline-Dept of Justice
202-697-0101	DEFENSE DEPT OPERATOR
202-737-9616	Jobsline-Fed Info Center
202-755-3203	Jobsline-Hud Dept
202-755-5055	Jobline-EPA
202-755-7395	HUD Newsline
202-899-02xx	Answering Service
202-965-2900	Watergate
203-242-6492	UNIV OF HARTFORD
203-242-6852	UNIV OF HARTFORD
203-527-0006	OVL111
203-771-3930	PIONEERS
206-527-0030	Reciever Open Tone
206-641-2381	Voice Of Chester,Tone 111
206-722-0008	USSR Cant Be called Rec.
212-246-7170	WYLBUR
212-369-5114	RSTS/E, SPENCE SCHOOL
212-369-7003	Zoning Rec
212-370-4304	COSMOS NY
212-394-1203	COSMOS NY
212-586-0897	DIRTY
212-598-7001	NY STATE COLLEGE
212-654-9977	??????
212-736-3377	RAPID DATA
212-777-7600	NY STATE COLLEGE
212-799-5017	ABC New York Feed Line
212-807-1257	CHELSEA SQUARE
212-947-7522	ITT DIALCOM NETWORK
212-976-2727	P.D.A.
212-986-1660	Stock Quotes
213-254-4914	Dial-A-Athiest
213-277-0174	UNKNOWN
213-331-0437	UNKNOWN
213-372-6244	Jokes
213-571-6523	SATANIC MESSAGES
213-642-2706	LYOLA COLLEGE
213-664-7664	Dial-A-Song
213-688-6694	Newsline- Govt Policy LA
213-742-8000	LAUSD
213-765-1000	LIST OF MANY NUMBERS
213-765-2000	JOKES
213-798-2000	FTS
213-840-3971	HOROWITZ
213-888-7636	DIAL-A-POEM
213-935-1111	Signusoid
214-224-1799	Polarity Reverser
214-336-5236	Signusoid
214-647-2996	Zip Code Information
214-651-1461	Data-Tel
214-691-9929	Pay Phone in SMU dorm
214-742-1195	AT/T
214-742-1354	BELL, SOUTHWESTERN
214-742-1637	BELL, SOUTHWESTERN
214-742-2636	NTRCHA (CREDIT CHECKING)
214-742-3189	VM370
214-742-3999	JOSKES
214-995-5000	Data-Tel
215-387-1129	UNKNOWN
215-563-9213	HP3000
215-564-6572	ATLANTIC CITY CASINO
217-429-9532	Dial-A-Prostitute
219-234-7121	Indiana Time
301-357-1452	Jobsline-Natl Oceanic Admin
301-496-1209	Jobsline-Natl Inst Of Hlth
301-881-6156	HP3000
301-881-6157	HP3000
301-881-6158	HP3000
303-232-8555	HP3000
303-299-1111	General Telephone Time
303-371-1296	JC PENNY CREDIT CARD
303-447-2540	RSTS/E, COCIS
303-499-7111	US BUREAU OF STANDARDS
303-978-2111	WANG VS/80
304-344-9811	Weather (Charleston)
304-346-1961	Extended Weather Charlston
304-348-9950	All carrier circuits busy
304-348-9951	All carrier circuits busy
304-348-9952	Improper Carrier Rec
304-348-9953	Code to be proceeded by 950
304-348-9954	950 Not Before Carrier Rec
304-348-9955	Polarity Reverser
304-348-9956	All Circuits Busy Rec.
304-348-9957	Technical Difficulty Rec.
304-348-9959	Carrier Code Not neccesary
305-973-8768	Pompano Park Horse Racing
305-994-2160	Data-Tel
305-994-2331	Fading Carrier
305-994-9960	Call Not Go Through Rec
305-994-9963	Payphone Inst. Rec
305-994-9964	IBM Reference Rec

"I have to admit these Feds are getting pretty clever"

Number	Description
312-222-6000	UNKNOWN
312-444-7777	ADS
312-645-7770	UNKNOWN
312-663-0884	Newsline- Govt Policy Chcgo
312-759-9191	Diversadial
312-792-1051	Dial-A-Trance
312-939-7950	DEPAUL
312-972-7603	ARROGON NET LAB
312-996-5100	TSO
313-234-5621	FTS
313-358-5780	UNINET
313-377-4300	OAKLAND UNIV
313-577-0260	WAYNE STATE
313-577-0266	MERIT TIMESHARING
313-644-3840	HIGH SCHOOL
313-644-3960	UNKNOWN
313-769-8803	W.I.T.S.
313-769-8821	ANN ARBOR SCHOOLS
313-839-3373	BELL, MICHIGAN
313-857-9500	OAKLAND SCHOOLS
313-881-0659	BELL, MICHIGAN, REPAIR COMP
313-892-0060	BELL, MICHIGAN
313-924-9977	BELL, MICHIGAN
313-961-8572	BELL, MICHIGAN, COs
313-962-1102	BOND-NET
313-962-1537	UNKNOWN
313-964-0042	BELL, MICHIGAN
313-964-2000	SEMAT COMPUTER
313-964-2018	CHARGE CARD ASSOCIATION
313-964-2064	ENGINEERING-SMITH/HENCHMAN
313-964-2500	UNIV OF KY
313-964-4042	BELL, MICHIGAN
313-964-5808	MICH NAT'L BANK
313-964-5858	LAW OFFICES
315-423-1313	SYRACUSE DECS
404-885-3460	SEARS CREDIT CHECK
405-843-7396	SYNTHACER MUSIC
408-280-1901	TRW
412-794-7601	SLIPPERY ROCK OIL
414-259-1233	RVS CABLEVISION
414-445-4050	DEC VAX
414-476-8010	DEC PDP-11/70, RSTS/E
414-542-4494	RSTS/E
414-543-0789	RSTS/E
414-543-4494	UNKNOWN
414-628-0001	Tone
414-628-0002/4	Tele-Copier
414-628-0006/7	Tele-Copier
414-628-0010/1	Muted Loop
414-628-0013/4	Inf Silence
414-628-0015	Tone & Silence
414-628-0017	2 clicks & silence
414-628-0028	Tone & Silence
414-628-0052	Special Operator
414-781-0004-7	Data-Tels
414-781-0010	Milliwatt
414-781-0014	Milliwatt
414-781-0015	Dial-Tone
414-781-002x	CO number
414-781-003x	CO number
414-781-004	CO number
415-327-5220	NEC
415-361-2500	MENLO PARK CORP.
415-367-3411	UNKNOWN
415-486-4959	DEVELCON
415-486-7015	UNIX
415-486-7020	UNIX #3
415-843-7439	DIAL-AN-EXCUSE
415-857-8193	HP3000
415-937-2868	UNINET
512-259-0004	Milliwatt
512-385-4170	HP3000
512-472-2181	WEIRD RECORDING
512-472-4263	Outside Wats Line Rec
512-472-9833	must 1st dial 1 or 0 rec
512-472-9936	not be completed rec
512-472-9941	"INSERT .25"
512-474-5011	AUSTIN COMPUTERS
515-294-9440	ISO
516-567-8013	LYRICS TIMESHizafG
516-586-2850	RSTS/E
516-794-1707	Stock Quotes
602-965-7001	ARIZONA STATE
606-257-3361	UNKNOWN
609-452-0025	UNIX
609-452-6736	PRINCETON
609-734-3131	RCA/CMS
609-799-7147	UNKNOWN VMS
612-333-0868	The "9" tone
612-333-1466	Facsimile Machine
612-333-1693	Tone Test
612-333-1705	Tone Test
612-333-1708	Tone Test
612-333-1743	Tone Test
612-333-1992	Tone Test
612-339-5200	INT'L GRAPHICS
612-473-9207	Odd Tone
617-258-8313	MIT
617-417-9203	NORTHEASTERN UNIV.
617-637-1234	Boston Time
617-732-1251	HARVARD
617-732-1802	HARVARD
619-485-9888	VAX 11/44
619-748-0002	1000 hz Tone
619-748-0003	Signusoid
619-748-0005	Pac-Bell Operator
703-781-4520	MERADCOM
704-847-1112	Milliwatt
704-847-1113	Open Circuit
713-483-2700	NASUA
713-792-7200	EDUCATIONAL RESEARCH
713-795-1200	SHELL VULCAN
713-881-8181	Houston Repair
714-598-4861	POLYTECH UNIV.
714-630-0003	Signusoid
714-630-9998	Polarity Reverser
714-638-3492	TRW
714-776-4511	TRW
714-891-1267	DIAL-A-GEEK
714-897-5511	General Telephone Time
714-956-3370	TRW
714-962-3365	H.A.T.S.
717-872-0911	MILLERSVILLE UNIVAC
718-273-9978	Continual Ring
718-338-4900	The Kook Line
718-526-1111	New York Feed Line
718-526-6019	Swammy
718-976-2727	P.D.A.
800-221-0226	NBA HOTLINE
800-221-2371	ADS
800-221-4945	Woman USA News
800-222-0248	Dow Phone
800-225-8456	AUTONET
800-228-1111	VISA CREDIT CHECK
800-228-8777	Zip Code Information
800-238-5342	National Cotton Council
800-242-4022	Smog Report In Los Angeles
800-248-0151	WHITE HOUSE PRESS
800-252-0112	USC NEWSLINE
800-253-9892	Up-Time Distribution
800-321-1082	NAVY FINANCE CTR.
800-321-3048	Beepers
800-321-3049	Beepers
800-321-3052	Beepers
800-321-3074	Beepers
800-325-0887	ARTS PROGRAM GUIDE
800-325-4072	COMBAT ARMS & SER ENLISTED.
800-325-4095	COMBAT SUPPORT BRANCH
800-325-4890	ROPD USAR COMBAT ARMS DIV.
800-325-9999	Strange Tone
800-327-6764	AUTONET
800-331-3701	Shell Credit Center
800-336-0149	Tymnet Offices
800-336-3366	The Source Customer Service
800-362-7171	MASTERCARD/VISA NO.
800-367-4710	Smog Report-San Bernando
800-368-5468	"Satellite Network Control"
800-368-5500	Coin Update
800-368-5634	MCI UPDATE
800-368-5640	Senate Update
800-368-5642	Nuclear Regulatory Comm. Op
800-368-5667	Business Line
800-368-5693	Republican Talk Line
800-368-5744	AFL-CIO News
800-368-5814	NTL ASSN OF REALTORS
800-368-5833	AM HERITAGE FOUNDATION
800-368-5844	Comm Satelite Corp
800-368-5939	White House Operator
800-424-0214	Ofc of Education News
800-424-2424	Am Fed of Teachers
800-424-5040	N.A.M. Newsline
800-424-5201	EXPORT IMPORT BANK
800-424-8086	Natl Ecucation Assn
800-424-8530	Housing & Urban Devlpmt
800-424-8807	TRANSPORTATION NEWSLINE
800-424-9090	White House Press Office
800-424-9128	DEPT OF ENERGY NEWSLINE
800-424-9129	IN SPANISH
800-424-9180	COMMANDER II
800-424-9440	COMMANDER II
800-424-9494	TELEMAIL
800-424-9820	Citizens Choice News
800-424-9864	Energy Line
800-426-5996	PUGET SD. NAVAL SHIPYARD.
800-432-3960	SOC.SEC.
800-521-8426	RSX-11
800-523-0677	ALCOHOL TOBACCO AND FIREARM
800-525-3056	Cattleman News
800-525-3085	Cattleman News
800-525-7623	Am Express Curr Exch Rt
800-528-2121	American Express voice crdt
800-532-1556	FED INFORMATION CTR
800-544-6363	Alliance Tele-Conference
800-548-0000	Chicago Announcement #2
800-562-0240	Metrophone Offices
800-621-7640	Sports Line
800-621-8094	American Medical Assn
800-622-0858	Calif Medical Assn
800-631-1147	Beepers
800-645-5350	UNKNOWN
800-645-5656	Sports Line
800-882-1061	AT&T Stock Prices
800-942-7071	BANK
806-741-5951	COLLEGE COMPUTER
806-741-6701	COLLEGE COMPUTER
815-633-6533	Diversadial
815-877-9521	Diversadial
816-221-9980	LOOP (TONE SIDE)
816-221-9984	LOOP (OTHER SIDE)
816-391-1122	Line Test #, hit tones
816-474-9982	DIAL TONE?
817-332-8491	FORTWORTH SCHOOL
817-338-0180	Ft. Worth Time & Temp
817-469-1895	Signusoid
817-469-4000/	Page-A-Fone's
817-469-4999	Page-A-Fone's
817-469-50xx	Mobile-Telephone-
817-469-51xx	Numbers
817-469-5200/	Page-A-Fone's
817-469-5999	Page-A-Fone's
817-625-6401	GIS
817-692-0537	WOODHILL MEDICAL
817-844-RITA	Ft. Worth Time & Temp
817-877-0548	RSTS/E
817-977-0663	AUTOBAHN IMPORTS
818-571-6523	The Gospel Line
818-702-0429	The Observatory
818-716-9242	...Input Line
818-761-3330	The Movie Line
818-765-1000	California Recordings
818-765-2000	Zygot Joke Line
818-765-6000	Feedback
818-765-7000	California Recordings
818-982-7000	Funfone
900-410-6272	SPACE SHUTTLE COMM.
904-644-2261	UNIV OF FLORIDA
914-268-9901	CC Verifacation
914-268-9911	deposit 5 cents rec
914-268-9913	deposit 10 cents rec
914-268-9936	Voice # to TelCo
914-268-9937	Voice # to TelCo
914-268-9960	Oscillating Tone
914-268-9963	Oscillating Tone
914-268-9966	Carrier
914-997-1277	Stock Quotes
916-445-2864	Gov of California

THIS LIST IS AVAILABLE ON THE 2600 SUBSCRIBER BULLETIN BOARD, SATURDAY AND SUNDAY MORNINGS FROM MIDNIGHT TO NOON (EASTERN TIME). PLEASE SEND US MORE NUMBERS SO WE CAN MAKE THIS LIST EVEN BIGGER.

SYSTEMATICALLY SPEAKING

Sprint Unites with US Telecom

Combined New Services

In the largest consolidation yet of the turbulent long-distance telephone industry, the nation's third and fourth largest services competing with AT&T—GTE-Sprint and US Telecom agreed to merge and form a new company.

This closely follows the proposed merger of MCI and SBS-Skyline which was announced last fall.

The creation of the US Sprint Communications Company, which faces Federal approval, will also merge their data communications subsidiaries, GTE Telenet and US Telecom Data Communications Company, which until a few months ago was know as Uninet.

Sprint and US Telecom will be able to combine their advertising and network-building efforts in the new company which will have a subscriber base of 2.2 million.

The new company would be the third largest long distance company, behind AT&T and MCI, and would be jointly owned by GTE and United Telecommunications.

Write Protect Tabs Wrong

Infoworld

If you are having data loss from a batch of floppy disks made by 3M, it is possible you have the red write-protect tabs it shipped with some of its disks last June and July.

The problem with the red tabs, used to cover the write-enable notch in floppy disks, is that they are transparent to the infrared light used by a few disk drives to check for the presence of the tab. While 3M said it has known about the problem since July, the company claims that the disks themselves are not defective. 3M will replace the red tabs if you contact the company.

One customer, who damaged his Microsoft Word and Smart Works program disks in January, called 3M's toll-free hotline [which is not listed with information] and had his disks replaced. He had Mitsubishi disk drives. About 1 percent of all disk drives will not detect the red tabs, according to a 3M spokesman.

Bell Atlantic & MCI Collaborate

Combined News Sources

As a result of the recent antitrust judgment against AT&T and the seven Bell operating companies, Bell Atlantic is signing up for MCI's long distance service. The switch won't affect customers since it's only intended for internal use of Bell Atlantic. Also, as part of the agreement, MCI is buying billing services from the local Bell Atlantic phone companies. This means that as of January 1, 1986, Bell Atlantic companies started sending MCI bills to MCI customers.

Cellular Phones in England

Newark Star Ledger

Cellular telephone users who travel overseas will soon be able to use the service in the United Kingdom.

Bell Atlantic Mobile Systems is setting up a reciprocal program with Cellnet of London, called Service Link, which will allow customers to pick up portable cellular telephones on their arrival at airports. Fees for the service have not yet been fixed.

Infrared Beeper Will Find You

USA Today

There's no escaping the infrared eyes of a new telephone beeper system. Telocall, from Teloc Inc., finds you virtually anywhere in a building and triggers a beeper that is worn like a pin. If you want to take the call, the system rings the nearest phone. If you don't, you press a button on the beeper.

When a call comes in, the sensors instantly search a room—much like an invisible flash bulb going off—and beep the person being called. The system is designed to locate as many as 1,000 individuals in 250 separate locations within a 50,000-square-foot office.

Electronic Tax Returns Are Here

InfoWorld

The Internal Revenue Service has announced that it will begin accepting 1985 tax returns in electronic form through approved tax preparation services.

The Electronic Filing Project, if successful, could eventually allow personal computer owners to file returns electronically, although not in the near future, according to a spokesman for the IRS.

The project could have a double advantage—for taxpayers, electronic filing may speed up the refund process; for the IRS, it may also reduce the cost of handling the millions of returns filed each year. Three areas have been selected for the initial test: Phoenix, Cincinnati, and the Raleigh-Durham and Fayetteville areas of North Carolina.

H&R Block Inc., of Kansas City, Missouri, is the first tax preparation service to announce participation in the IRS project. Customers of designated offices can use H&R Block's Rapid Refund service.

Other tax preparation services are being considered by the IRS to participate in the project, but those preparers must first pass transmission tests in order to be certified.

H&R Block prepares more than 9 million tax returns a year, or about 10 percent of the individual returns filed in the country.

Acoustic Trauma

The New Brunswick Home News

On Father's Day this year, an 18-year-old Scotch Plains, New Jersey man was talking on a telephone and experienced what he believed was an electrical shock.

An investigation by AT&T and New Jersey Bell later revealed that the young man was an "acoustic trauma" victim.

Phone company officials describe acoustic trauma as "a pop or a click" that can sound as loud as the backfire of an automobile.

Like many victims of acoustic trauma, the man suffered no serious injuries but had a ringing sensation in his ears for about a day.

A New Jersey Bell spokesman said acoustic trauma is not the same thing as an electrical shock.

"The telephone converts electrical currents into sound waves," he said. "Acoustic trauma comes as a result of sound waves, and not electrical currents."

Devices known as "acoustic filters" are built into telephone receivers and are designed to minimize the clicking noises that sometimes result from malfunctions within a telephone network.

One or two cases of acoustic trauma are reported to AT&T each year.

DIAL BACK

modem into believing that it is seeing dial tone, ringback and so forth until he supplies answerback tone and connects and penetrates the system, security should not depend on this sort of dial-back.

The best thing to do to solve this problem is to use a different line for dial-out. Use of random time delays between dial in and dial back combined with allowing the modem to answer during the wait period (with provisions made for recognizing the fact that this wasn't the originated call - perhaps by checking to see if the modem is in originate or answer mode) will substantially reduce this window of vulnerability but nothing can completely eliminate it.

Obviously, if one has an older CO switch, it is not good at all to use the same line for dial in and dial out.

It is best to make sure that the phone number for the dial out is different from that of the dial-in, perhaps even in a different exchange, which isn't all that impossible.

```
2600 BBS
For the latest in
     news on the
   Private Sector
and a chance to
communicate with
        other
   subscribers!

OPEN SATURDAY AND
SUNDAY, MIDNIGHT
TO NOON, EASTERN
TIME
NO PASSWORD
REQUIRED THIS
MONTH ONLY!
516-751-2600
```

MAIL

Dear *2600*:

I have a great idea, which seems so simple, but I have never heard anyone mention it. It concerns protecting the userlog of a BBS from the prying eyes of the Gestapo police, or FBI, or whoever.

You see, when they raid your house to take your BBS, they have only a few reasons. It is either to punish you for asking questions or to get a juicy list of people to investigate along with their favorite passwords. Sometimes they will call up other boards using the user names and passwords they just confiscated and try to read personal mail. This strikes me as being both immoral and illegal. But anyway, the trick is to not have the userlog available.

I have solved this problem by putting the userlist in memory on a ram-disk. I have a simple program which makes my computer think that part of the memory is really a disk that you can write to or read from. When the cops come racing in and pull the plug in an attempt to confiscate my computer, the information is gone. It just disappears. The only problem is that you need a computer that has more than 64K, like a PC or something, because most programs need 64K of available memory to run.

It is unlikely that they will try to probe your computer before they unplug it and take it from your home "as evidence," because even their technical people are pretty incompetent. And they don't usually send their technical people along anyway. I am pretty sure of that, because they like to take calculators and normal telephones along with the computer, and that shows an extreme lack of knowledge.

Since the BBS is almost always on, the userlog can be backed up on a disk outside of the computer, but encrypted in some way. All you have to do is scramble it, then rename it and put it in the middle of your Basic programs or wherever. No one but the NSA would find it. And they have better things to do...

Mojave Dessert