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 819 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 6600 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

User Name: NCR508LOD
Password: LOD/H Network Communications Resources

VAX/VMS Version 4.2

Last Interactive logon on Wednesday, 01-JUN-1985 10:20:11
Last noninteractive logon on Friday, 30-MAY-1985 15:30:27
2 failures since last successful login
You have 1 new mail message
5

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. It is also 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.

User Name: Password: RJE HOST LINK INFO BACKUP NETWORK DF MAIL DENT PHRYS 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 be user selectable. The rights list is the structure that VMS uses to perform all protection checks. 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. This will allow you to control your connection. Subprocess logins are always 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. 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.

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 media is always audited by a subject attempting to gain access to an object. VMS ensures that access is being centrally controlled, and that the security manager is given the right to control access. 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 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 the 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 losses. The encryption system included in the operating system is much easier to crack than those few that are motivated. The encrypt facility does not use a sufficiently complex algorithm to be unbreakable. Unfortunately, it would stifle slow evolution of code.

Internal Security

VAX/VMS determines access to objects by utilizing two protection mechanisms: Access Control Lists (ACLs), and User Identification Codes (UIDs). 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) UICs that identify each user on the system; 2) General identifiers are defined by the security manager in the system rights database to identify groups of users based on their use of the system. An ACL consists of one or more Access 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. There are access types: 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 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 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 it can halt a user's process. Of course, the log system function 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 written to the console. Someone who has such a privilege is usually 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's 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. 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's 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.

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

(continued on page 3-16)
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

Associated Press

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

Associated Press

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.
THIS MONTH’S MAIL

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 thing 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.

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.

(continued on page 3-16)
The 2600 Information Bureau

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, The Kid & Company, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

I have to admit these Feds are getting pretty clever
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 known 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.

Infrared Beeper Will Find You

USA Today

There's no escaping the infrared eyes of a new telephone beeper system. Telocal, 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

(continued from page 3-10)

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.

MAIL

(continued from page 3-12)

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 Desert

FULL DISCLOSURE

is the most amazing newspaper available

Do you know what is really going on in the world today? When you read your daily newspaper you only get part of the story. In the book Media Monopoly, Tom Phillips described it this way:

"Authorities have always recognized that to control the Public they must control information. . . . By 1950, the majority of all major business media. . . were controlled by 50 giant corporations. Thus corporations were centralized in enormous financial unions with other economic industries and with a few dominant international banks. . The men and women who held these corporations. . . constituted a "Public Authority of Information and Culture.""

Full Disclosure is a completely independent monthly paper that publishes information you need to know, information you won't find in your daily newspaper. Do you only want to know what 50 giant corporations find suitable for you? Or do you want a unique and often suppressed viewpoint?

It is certain that Full Disclosure fills a gap within our society. There is a need for a publication that throws light on the activities of governmental organizations that form a state within a state. Since the first edition of Full Disclosure welcomed its readers about abuses, evil and unlawful activities of governmental departments. Full Disclosure has certainly become recognized by the offended, the fourth power in our society.

Full Disclosure reader K.M. of Knoxville, TN recently wrote: "I am really impressed! You wouldn't believe how many things I've subscribed to, looking for this, but was usually disappointed because of the lack of depth. I would never have found out this stuff if subscribed to the full disclosure..."

Now you don't have to dig through the publication programs to find Full Disclosure. You can just fill out the order coupon below and return it to Full Disclosure now.

Please enter your subscription to Full Disclosure for:

| | Sample (1 issue) | $1.95 | 1 year (2 issues) | $14.00 | 2 years (24 issues) | $26.95 |
|---|---|---|---|---|---|
| Name | | | | | |
| Address | | | | | |
| City/State/Zip | | | | | |
| Payment Method | | | | | |
| Full Disclosure, P.O. Box 679-28, Ann Arbor, Michigan 48107 |
| Notes: our offices are located at 294 South Main St, Ann Arbor, Michigan. (Businesses, out advertising rate and is available upon request)