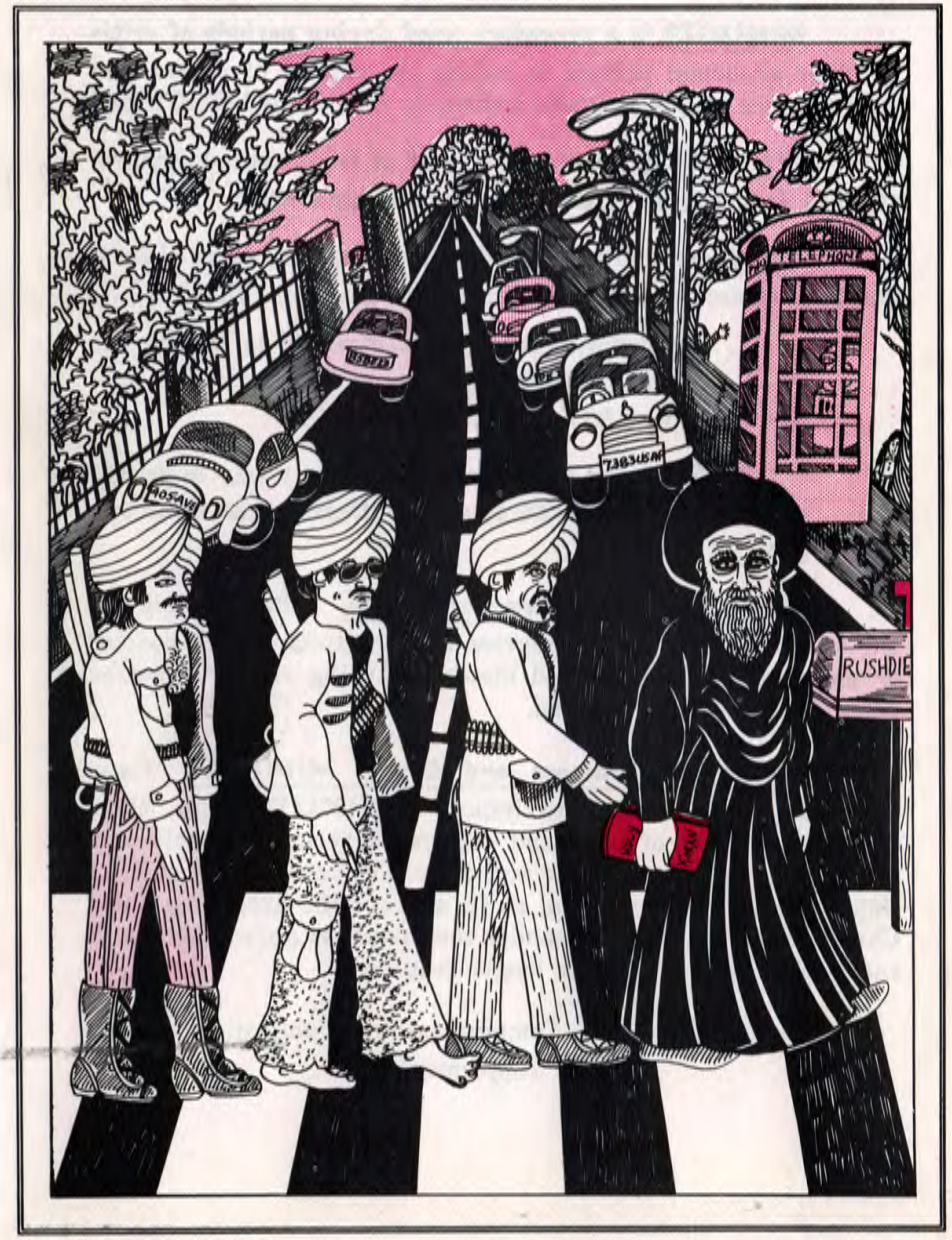
2600

The Hacker Quarterly

VOLUME SIX, NUMBER ONE
SPRING, 1989



MINIMIZE

MINIMIZE is a procedure used during periods of crisis or other abnormal periods to reduce the volume of record and long distance telephone traffic ordinarily transmitted electrically.

MINIMIZE applies to ALL users of DOD communications systems, including originators of card and tape traffic.

Procedures. When MINIMIZE is imposed, users of DOD electrical communications facilities must determine that:

1. The information to be forwarded is required to avoid a seriously detrimental impact on mission accomplishment or safety of life.

2. Electrical transmission is the only way to get the information to the addressee in sufficient time to accomplish its purpose.

Alternate Means of Communications. The US mail, the US Armed Forces Courier Service, or an individual as a courier or messenger should be used instead of using electrical means when MINIMIZE is imposed.

Authority to Impose and Cancel MINIMIZE. Commanders are authorized to impose MINIMIZE within their command or area of command responsibility unless specifically denied by appropriate higher authority. The Joint Chiefs of Staff impose it worldwide as well as in any specific area. The Joint Chiefs of Staff or the commander concerned, as appropriate, will cancel MINIMIZE when no longer required.

Authority. Allied Communications Publication (ACP) 121 US Supplement-1

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987
at $25 per year, $30 per year overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.

***2600* Office Line: 516-751-2600**

HACKERS IN JAIL

Story Number One: By now we've probably all heard about Kevin Mitnick. Late last year, this computer hacker was arrested after being turned in by his friend, who explained it all by saying, "You're a menace to society."

Mitnick has been described in the media as 25, an overweight, bespectacled computer junkie known as a "dark side" hacker for his willingness to use the computer as a weapon. His high school computer hobby was said to have turned into a lasting obsession.

He allegedly used computers at schools and businesses to break into Defense Department computer systems, sabotage business computers, and electronically harass anyone -- including a probation officer and FBI agents -- who got in his way.

He also learned how to disrupt telephone company operations and disconnected the phones of Hollywood celebrities such as Kristy McNichol, authorities said.

Over the past few months, several federal court judges have refused at separate hearings to set bail for Mitnick, contending there would be no way to protect society from him if he were freed.

Mitnick's family and attorney said prosecutors have no evidence for the accusations and that they are blowing the case out of proportion, either out of fear or misunderstanding of the technology.

Mitnick has an amazing history, to say the least. He and a friend logged into a North American Air Defense Command computer in Colorado Springs in 1979. The friend said they did not interfere with any defense operation. "We just got in, looked around, and got out."

Computer security investigators said that as a teenager Mr. Mitnick belonged to a shadowy Southern

(continued on page 20)

MORE ON

by Red Knight
Phreakers/Hackers Underground Network

This is the conclusion of a two-part article. Part One appeared in our last issue.

More UNIX Commands

man [command] or **[c/r]** - will give you help for a command.

help - available on some UNIX systems.

mkdir [dir name(s)] - makes a directory.

rmdir [dir name(s)] - removes a directory. You won't be able to remove the directory if it contains files.

rm [file name(s)] - removes files. rm * will erase all files in the current directory. Be careful! Some options are: [-f unconditional removal] [-i prompts user for y or n].

write [login name] - to write to other logged in users. Sort of a chat.

mesg [-n] [-y] - doesn't allow others to send you messages using the write command. Wall used by system adm overrides it.

$ [file name] - to execute any file.

wc [file name] - counts words, characters, lines in a file.

stty [modes] - set terminal I/O for the current devices.

sort [filename] - sorts and merges files -- many options.

spell [file name] > [file name] - the second file is where the misspelled words are entered.

date [+%m%d%y*] [+%H%%M%S] - displays date according to options.

at [-r] [-l] [job] - does a specified job at a specified time. The -r removes all previously scheduled jobs. The -l reports the job number and status of all jobs scheduled.

write [login] [tty] - sends a message to the login name.

su [login name]

The su command allows one to switch users to a super user or to another user. Very important -- could be used to switch to super user accounts.

$ su sysadm
password:

This su command will be logged in /usr/adm/sulog and this file of all files is carefully monitored by the system administrator. Suppose you hacked into john's account and then switched to the sysadm account. Your /usr/adm/sulog entry would look like this:

SU 04/19/88 21:00 + tty 12 john-sysadm

Therefore the S.A. (system administrator) would know that john switched to the sysadm account on 4/19/88 at 21:00 hours.

"Do not use login names like Hacker, Cracker, Phreak, etc."

Searching For Valid Login Names

Type in:

$ who (this command informs the user of other users on the system)

cathy tty1 april 19 2:30
john tty2 april 19 2:19
dipal tty3 april 19 2:31

tty is the users terminal The date and time shown are those of their logins.

/etc/passwd File

The etc/passwd is a vital file to cat.

It contains login names of all users including super user accounts and their passwords. In the newer SVR3 releases security is tightened by moving the encrypted passwords from /etc/passwd to /etc/shadow which makes it only readable by root. This is optional, of course.

```
$ cat /etc/passwd
root:D943/sys34:0:1:0000:/:
sysadm:k54doPerate:0:0:administration:usr/admin:/bin/rsh
checkfsys:Locked;:0:0:check file system:/usr/admin:/bin/rsh
john:chips11:34:3:john scezerend:/-usr/john:
$
```

If you have reached this far, capture this file as soon as possible. This is a typical output of an etc/passwd file. The entries are separated by a ":". There may be up to seven fields in each line. Let's look at the "sysadm" example. The first field has the login name, in this case sysadm. The second field contains the password. The third field contains the user ID ("0" is the root). Next comes the group ID and then the account which contains the user's full name, etc. The sixth field has the login directory which defines the full path name of the particular account and the last field contains the program to be executed. The password entry in the field of the checkfsys account in the above example is "Locked;". This means that the account checkfsys cannot be accessed remotely. The ";" acts as an unused encryption character. A space is also used for this purpose. You will find this in many small UNIX systems where the system administrator handles all maintenance.

Password Aging

If password aging is active the user is forced to change the password at regular intervals. One may be able to tell just by looking at the /etc/passwd file when the password is allowed to be changed and when it is compulsory to change it. For example, the entry:

john:chips11,43:34:3:John Scezerend:/usr/john:

The password contains an extension of (,43) which means that john has to change the password at least every six weeks and can keep it for at least three weeks. The format used is [password],Mmww. The M is the maximum number of weeks before the password has to be changed and m is the minimum period before the password can be changed. The ww indicates when the password was last changed.

Aging chart:

Character	# of weeks
.	0
/	1
0-9	2-11
A-Z	12-37
a-z	38-63

From the above, anyone can determine the number of weeks when one can change the password. The "ww" is automatically added telling when the password was last changed.

If Shadowing is Active

If the shadowing is active the /etc/passwd will look like this:

```
root:x:0:1:0000:/:
sysadm:x:0:0:administration:/usr/admin:/bin/rsh
```

The password is substituted by "x". The /etc/shadow file is only readable

by root and will look similar to this:

root:D943/sys34:5288::
Cathy:masai1:5055:7:120

The first field contains the user's ID. The second contains the password. The password will be NONE if remote logins are deactivated. The third contains a code of when the password was last changed. The fourth and the fifth contain the minimum and the maximum number of days for password changes. (It's rare that you will find this in the super user logins due to their hard-to-guess passwords.)

/etc/options Directory

The etc/options directory will consist of utilities available in the system. For example:

-rwxr-xr-x 1 root sys 40 april 1:00 uucp.name

/etc/group

The file has each group on the system. Each line will have four entries separated by a ":". An example of concatenated /etc/group:

root::0:root
adm::2:adm,root
bluebox::70:

The format is: group name:password:group ID:login names. It's very unlikely that groups will have passwords assigned to them. The ID "0" is assigned to "/".

Sending and Receiving Messages

Two programs are used to manage this. They are mail and mailx. The difference between them is that mailx is fancier and gives you many choices like replying, using editors, etc.

The basic format for sending mail is:

$ mail [login(s)]

(Now one would enter the text. After finishing, enter "." (a period) on the next blank line.)

This command is also used to send mail to remote systems. Suppose you wanted to send mail to john on a remote called ATT01. You would type in:

$ mail ATT01!john

Mail can be sent to several users just by entering more login names after issuing the mail command.

Using mailx is the same basic format.

$ mailx john
subject: (this allows you to enter the subject)
(line #1)
(line #2)

(After you finish, enter "~.". More commands are available like ~p, ~r, ~v, ~m, ~h, ~b, etc.)

After you logon to the system, your account may have mail waiting. You will be notified "You have mail". To read it enter:

$ mail
(line #1)
(line #2)
(line #3)
?
$

After the message you will be prompted with a question mark. Here you have a choice of deleting the message by entering "d", saving it to view it later by entering "s", or just press enter to view the next message.

Super User Commands

sysadm adduser - will take you through a routine to add a user.

Enter this:

$ sysadm adduser
password:

(this is what you will see)

Process running subcommand

GENERAL INFORMATION

USE OF OFFICIAL TELEPHONES FOR PERSONAL BUSINESS

Telephones are not to be used by employees for personal messages except in case of emergency. Use pay stations located in convenient places in all buildings. Chief of Bureaus are expected to cooperate in securing strict observance of this instruction and each person having a telephone on his or her desk is responsible for its proper use.

ALL NUMBER CALLING EXCHANGES FOR THE DEPARTMENT OF DEFENSE

Be sure you have the correct number in mind. Consult the directory. Listen for dial tone and then dial the number.

69.2—69.3—69.4—69.5—69.6—69.7

When calling from one of the above exchanges to another one of the above exchanges dial only the last 5 digits of the number.

When calling from one of the above exchanges to an entirely different exchange in the Metropolitan Area not listed above, dial 9 and listen for dial tone*, then dial all 7 digits.

*(This dial tone will be continuous and will sound the same as the original dial tone. Please continue dialing).

The prefix for all 8 digit telephone numbers appearing in the DoD directory is "69".

AUTOMATIC VOICE NETWORK (AUTOVON)

Numbers listed in this directory are not autovon.

The Automatic Voice Network (AUTOVON) is the basic General Purpose switched voice network of the Defense Communications System. Autovon serves most major installations in CONUS and limited overseas areas. To avoid abuse of the Network and derive maximum efficiency users must be familiar with the system and cooperate fully. You can assist by following these guidelines.

Consult the AUTOVON listings in this directory or dial "O" for up-to-date information.

Send a message instead. Use AUTOVON only when your communications requires a time sensitive reply.

Restricted lines cannot be used to place AUTOVON calls.

Don't use AUTOVON for unofficial business. Unless the communication is official and essential and would stand the scrutiny afforded a commercial toll call, AUTOVON should not be used.

Keep the call short. Policy on AUTOVON use states that calls should be no more than approximately 5 minutes in duration. Outline your communication prior to making a call and then limit it to 5 minutes. If you are seeking information which is not readily available, ask the party on the other end to call back.

Avoid system saturation. Most AUTOVON calls from the DC area are attempted in the middle of the morning or afternoon. When this happens there simply are not enough circuits to handle every call. Attempt to place calls throughout the day. Many calls are completed faster with less preemption in the early morning or late afternoon when there is less competition for circuits. AUTOVON access (CONUS only) Dial "9" listen for dial tone, then AUTOVON number.

AUTOVON access to overseas is not available through the DTS-W system. Overseas calls must be placed through the appropriate military switchboard serving your activity or by commercial means.

If you reach a busy signal (60 IPMS) on the number called, hang up and redial. If you reach a fast busy signal (120 IPMS), this indicates that the local or network equipment is busy. Hang up try again later.

Preemption—your call was cut off by a higher precedence call. Hang up and dial again.

Provide callers with your proper prefix for the Autovon calls. Washington area numbers listed in this directory are not Autovon numbers. See page 14 for cross-reference information.

LONG DISTANCE TELEPHONE CALLS

For calls within CONUS and to Hawaii, Puerto Rico, and the U.S. Virgin Islands.

Facilities are maintained within the Department of Defense for the most economical and efficient placing of long distance calls. To keep costs at a minimum, military departments must insure that only official calls of short duration be made over the Department of Defense facilities.

1. Applies to calls from *Unrestricted* telephone numbers only.
2. To place an official long distance call, dial 9 plus the area code and telephone number desired.
3. Avoid system saturation. Most Long Distance calls from the DC area are attempted in the middle of the morning or afternoon. When this happens there simply are not enough circuits to handle every call. Attempt to place calls throughout the day. Many calls are completed faster in the early morning or late afternoon when there is less competition for circuits.
4. If a "circuits busy" recording is encountered, hang up and try your call later.
5. If the call is of such urgency that delays cannot be tolerated dial the Defense operator ("O") and tell her/him of the circuit busy condition and request her/his assistance.
6. Agencies will be provided a monthly statement of long distance usage which will include calling number, date, time connected, length of call (in minutes), cost of the call, state, and telephone number called.
7. These procedures do not apply to 437 (Reston), or 756-5xxx (Melpar) exchanges.
8. Calls to Long Distance Information i.e. (Area + 555-1212) should be placed via the DoD Telephone Operator (Dial "O").
9. Calls to Area Code "800" may be dialed direct from any DOD telephone. Calls to Area Code "800" are free.
10. Refer to page 8 for Area Code numbers most frequently called.

CONFERENCE CALLS

1. Conference Calls established for DTS-W Telephone Users via the DoD Operator can consist of a maximum of twenty two parties local, CONSUS Long Distance and/or Overseas.
2. Conference Calls established for DTS-W via the "Meet Me" feature can consist of a maximum of twenty two parties, Local, CONSUS Long Distance and/or Overseas. The "Meet Me" feature allows conferees to dial directly into the conference automatically at a pre-determined time without operator assistance.
3. To arrange a conference call, dial "O", ask for the DoD Conference Operator and provide the following information:
   a. Your Name—DoD Telephone Number—DoD Agency.
   b. Date/Time/Approximate duration of conference.
   c. Names/Area Code + digit numbers of conference.
   d. Whether the teleconference will be operator-assisted or dialed direct ("Meet Me").
   e. DoD Telephone Number to be billed (if operator assisted).
4. Since the Autovon network has lines conditioned for preemption, its use on the conference system is discouraged.
5. Conference Call Checklist.
   a. Before the teleconference, the meeting leader should send each participant the following:
      - Time/Zone and location of teleconference.
      - Agenda.
      - Visuals, Charts, Graphs.
      - List of Participants.
   b. The leader should contact all participants and arrange for each participant or a proxy to answer the telephone at the pre-determined time.
   c. During the teleconference, the leader should:
      - Announce the agenda.
      - Have participants introduce themselves.
      - Establish speaking order.
   d. Avoid use of extension telephone.

DOD OFFICIAL TELEPHONE CREDIT CARD USERS

Telephone credit cards are intended for official use when the authorized credit card holders is away from their permanent duty station and has a requirement to place an official call.

Credit cards will not be used by DOD officials to make calls from their permanent duty station.

TRANSFERRING CALLS*

IMPORTANT: To transfer a call, signal operator by pressing switch hook firmly ONCE.

You can transfer any incoming long distance or direct in-dialing call by signalling the operator. This transfer cannot be made if more than one telephone is open on the line attempting the transfer. Calls made to you from within the same exchange cannot be transferred.

*NOTE: Telephone users in the 286, 427, and 978 exchanges see instructions next page.

`adduser`
USER MANAGEMENT

Anytime you want to quit, type "q".
If you are not sure how to answer any prompt, type "?" for help.
If a default appears in the question, press <RETURN> for the default.
Enter user's full name [?,q]: (enter the name you want)
Enter user's login ID [?,q]: (the ID you want to use)
Enter user's ID number (default 50000) [?,q) [?,q]: (press return)
Enter group ID number or group name: (any name from /etc/group)
Enter user's login home directory: (enter /usr/name)

This is the information for the new login:
User's name: (name)
login ID: (ID)
users ID: 50000
group ID or name:
home directory:/usr/name
Do you want to install, edit, skip [i,e,s,q]? (enter "i" to install)
Login installed
Do you want to give the user a password? [y,n] (it's better to enter one)
New password:
Re-enter password:

Do you want to add another login?

This is the process to add a user. Since you hacked into a super user account, you can make another super user account by doing the following: enter 0 as a user and a group ID and enter the home directory as /usr/admin. This will give you as much access as the sysadm account. Caution: Do not use login names like Hacker, Cracker, Phreak, etc. This is a total giveaway. The process of adding a user won't last very long. The S.A. will know when he checks out the /etc/passwd file.

sysadm moduser - this utility allows one to modify users. Do not abuse!

Enter this:
$ sysadm moduser
Password:
(This is what you will see)
MODIFYING USER'S LOGIN

1) chgloginid (This is to change the login ID)
2) chgpassword (Changing password)
3) chgshell (Changing directory. DEFAULT = /bin/sh)

ENTER A NUMBER, NAME, INITIAL PART OF NAME, OR ? OR <NUMBER>? FOR HELP, Q TO QUIT

Try every one of them out. Do not change someone's password. It creates havoc. If you do decide to change it, write the original one down somewhere and change it back. Try not to leave too many traces after you have had your fun.

sysadm deluser - this is used to delete a user.

Enter this:
$ sysadm deluser
Password:
(This will be the screen output)
Running subcommand 'deluser' from menu 'usermgmt'
USER MANAGEMENT

This function completely removes the user, their mail file, home directory, and all files below their home directory from the machine.

Enter login ID you wish to remove [q]: (cathy)
'cathy' belongs to 'Cathy Franklin'
whose home directory is /usr/cathy
Do you want to remove the login ID 'cathy' ? [y,n,?,q]: (y)

/usr/cathy and all files under it have been deleted.

Enter login ID you wish to remove [q]:

Other Super User Commands

wall [text] control-d - sends an announcement to users logged in (will override mesg -n command). Execute only from /.
/etc/newgrp - used to become a member of a group.
sysadm delgroup - deletes groups.
sysadm diskuse - shows free space, etc.
sysadm whoson - self-explanatory.
sysadm lsgroup - lists groups.
sysadm mklineset - hunts various sequences.
sysadm lsuser - lists all the users and their login names.

Basic Networking Utility (BNU)

The BNU is a unique feature in UNIX. Some systems may not have this installed. BNU allows you to communicate with other remote UNIXes without logging off the one you're presently on. BNU also allows file transfers between computers. Most UNIX System V's will have this feature installed.

The user programs like cu, uux, etc. are located in the /usr/bin directory.

Basic Networking Files
/usr/lib/uucp/[file name]

systems - cu command to establish link. It contains info on the remote computer's name, the time it can be reached, login ID, password, telephone numbers, etc.
devices - interconnected with systems file. Also contains baud rate, port, etc.
dialcodes - contains abbreviations for phone numbers that can be used in the systems file.

Other files are dialers, sysfiles, permissions, poll, devconfig.

BNU Administrative Files

There are five administrative files present. These files are created in the /usr/spool directory. They are responsible for various BNU processes.
TM - this file is used to hold temporary data. When transferring the files from a remote to local the /usr/spool/uucp/[name of the remote computer] creates this in the following format: TM [Process Identification Number].[ddd]. The ddd is a 3 digit number (sequential) starting with "0". A typical example would be: TM322.012. This file is then moved into the path defined by the C.sysnxxx file.
X - executes files. Created in the /usr/spool before you execute the commands in remote. The format used to name this file is X.sysnxxxx where sys stands for the remote name and n is the priority level. The xxxx is a

"BNU allows you to communicate with other remote UNIXes without logging off the one you're presently on."

sequence assigned by the uucp. These files always contain the name of the file, computer and file name to receive, person's login and computer name, and the command string.

LCK - the lock file created in the /usr/spool/locks directory. This is used when devices are being used. Prevents usage of the same calling device. Format used: LCK.str where the str is a device name. The lock file contains the PID needed to lock.

C.sysnxxx - created in the usr/spool directory. These are the work files. Used when work is in line for remote executions. The format is the same as the X.sysnxxxx. The work files contain the full path name of the file to be sent, path name of the destination (TM Transfers), remote login name to be notified after the file transmission is complete, user's login name, and the name of the programs used (uucp, uupick, etc.).

"Do not change someone's password. It creates havoc."

D - the data files. Format used is D.systmxxxxyyy. These files are created when specified in a command to copy to the spool directory. The "systm" is the remote name, xxxx are the four digits sequentially assigned by the uucp. The yyy is a sub sequence number.

Logging Onto Remote and Sending, Receiving Files

cu - this command allows one to logon to the local as well as the remote UNIX (or a non UNIX) without having to hang up. This is useful for transferring files.

$ cu [-s baud rate][-o odd parity][-e even parity][-l name of comm line] telephone number | systemname

To view system names that you can communicate with, use the 'unname' command.

$ cu -s300 3=9872344 (9872344 is the telephone number)
connected
login:
password:

Local Strings

~. - will log you off the remote terminal but not the local.

~! - will log you off on the local without disconnecting the line from the remote.

<control-d> - puts you back on the remote UNIX.

~%take [file name] - takes a copy of the file name and copies it to the local (the directory which you are in).

~%put [file name] - reverse of above.

~$[command] - allows the execution of a command to the local from remote.

ct

ct allows the local to connect to the remote. Initiates a getty on a remote terminal. Useful when using a remote terminal.

$ ct [-h prevent automatic hang up][-s bps rate][-wt set a time to call back abbreviated t mins] telephone number

uux

To execute commands on a remote (UNIX to UNIX)

$ uux [- use standard output][-n prevent mail notification][-p also use

standard output] command-string

uucp

uucp copies files from one's computer to the home directory of a user in a remote system. This also works when copying files from one directory to another in the remote. The remote user will be notified by mail. This command becomes useful when copying files from a remote to your local system. The uucp requires the uucico daemon to call up the remote and to perform file login sequence, file transfer, and notification of the user by mail.

Daemons are programs running in the background. The three daemons in a UNIX are uucico, uusched, and uuxqt.

uuxqt - remote execution. This daemon is executed by uudemon.hour started by cron. uuxqt searches in the spool directory for an executable file named X.file sent from the remote system. When it finds the file it obtains the processes which are to be executed. The next step is to find out if the processes are available at the time. If they are it checks permission and if everything is OK it proceeds to the background process.

uucico - this daemon is very important. It is responsible for establishing a connection to the remote. It also checks permission, performs login procedures, transfers, and executes files. It also notifies the user by mail. This daemon is called upon by uucp, uuto, uux commands.

uusched - this is executed by the shell script called uudemon.hour. This daemon acts as a randomizer before the uucico daemon is called.

Usage of uucp Command

$ uucp [options] [full path name] file [destination path] file

Example:

$ uucp -m -s bbss hackers unix2!/usr/todd/hackers

What this would do is send the file hackers from your computer to the remote's /usr/todd/hackers. todd would get mail that said that a file had been sent to him. unix2 is the name of the remote.

Options for uucp:

-c don't copy files to spool directory

-C copy to spool

-s [file name] - this file will contain the file status (above is bbss)

-r don't start the comm program (uucico) yet

-j print job number (for above unix2e9o3)

-m send mail when file is complete

Now suppose you wanted to receive a file called kenya which is in the usr/dan/usa directory to your home directory /usr/john. Assuming that the local system's name is ATT01 and you are currently working in /usr/dan/usa, you would type in:

$ uucp kenya ATT01!/usr/john/kenya

uuto

The uuto command allows one to send a file to a remote user and can also be used to send files locally.

$ uuto [file name] [system!login name] (omit system name if local)

Conclusion

There's always more to say about UNIX but this is enough for now. I hope I have made the UNIX operating system a little more familiar. The contents of this article are all accurate to the best of my knowledge.

Remember not to abuse any systems you hack into. A true hacker doesn't like to wreck but prefers to learn.

ever wonder who owns

by Scott Statton
@ The TELECOM DIGEST

800 service is offered by various IECs. Each NXX in the 800 SAC is assigned to a given carrier, who is responsible for assigning numbers from that block to customers, and providing 10 digit translation. When you as Joe Customer dial 1-800-222-1234 (made up number, please don't bother them) it will initiate the following sequence:

1. If you are in an Electronic Office (DMS-100, DMS-200, 1A ESS, #5 ESS) the 800-222 will be translated to "AT&T" and search for an opening in a trunk group marked for 800 origination. Should none be found, bump to step 3.

2. If you are in a non-electronic office (SXS, XB, and some flavors of ESS), it will go to the access tandem that you're office "homes" on, where 800-222 will be translated to "AT&T".

3. Find a trunk in a trunk group marked for 800 origination. Should none be found, give the customer a recording "Due to network congestion, your 800 call could not be completed" or die, or whatever. (Depends on phase of moon, etc.)

4. The end office will then send the following pulse-stream (in MF):

KP + II + 3/10D + ST + KP + 800 222 1234 + ST

(note that this is a simplification, there are some fine points of ANI spills that are beyond the scope of this article)

II = 2 information digits ... typical values are:
00 normal ANI .. 10 digits follow
01 ONI line ... NPA follows
02 ANI failure ... NPA follows
3/10D = 3 or 10 digits. Either the NPA, or the entire 10 digit number.
KP and ST are control tones.

5. The carrier receives all of this (and probably throws the ANI into the bit bucket) and translates the 800 number to what's called a PTN, or Plant Test Number. For example, 617-555-9111. Then, the call is routed *as if* the customer had dialed that 10 digit number. Of course, the billing data is marked as an 800 call, so the subscriber receiving the call pays the appropriate amount.

800 Service and OCN Translation Table

Under Equal Access, any long distance company can carry 1-800 traffic. Which carrier gets the call is determined (at the moment) by the NNX of the number. 1-800-528-1234 is carried by AT&T while 1-800-888-1800 is carried by MCI.

The carrier must have Feature Group D presence for originating calls from the originating exchange (either direct, or through an access tandem).
In the future, when CCIS becomes wide-spread, a query will be made in the database [Who gets 1-800-985-1234?] and the call will be routed appropriately. To clarify: Now the carrier is determined by the NXX. In the future, the carrier will be determined by the entire

all those 800 numbers?

seven digits.

A similar situation exists with 900 service. Each carrier can reserve NXX's from BellCore (the people who among a zillion other tasks are in charge of handing out prefixes and area codes). They're not cheap! To get the actual number is free (when you meet certain qualifications), but to get it "turned on" in a LATA costs you money, depending on (1) how many prefixes you're getting, (2) whether it's 800 or 900 service, (3) how many tandems/end offices are in the LATA. It requires a discrete amount of labor for *each* office, because *each* routing table must be modified.

Of the 800 possible NXX's, 409 are currently assigned. A long distance carrier can get one 800 and four 900 numbers just for the paperwork. But to get more than that, you have to show that you're 70% full now, and demonstrate a real need for the capacity.

I have included the entire 800-NXX to long-distance carrier translation table. Note that not every NXX is valid in every area.

Revised 800/OCN Translation Table
Effective 10 October 1988

221 ATX	222 ATX	223 ATX	224 LDL	225 ATX
226 MIC	227 ATX	228 ATX	229 TDX	230 NTK
231 ATX	232 ATX	233 ATX	234 MCI	235 ATX
236 SCH	237 ATX	238 ATX	239 DLT	240 SIR
241 ATX	242 ATX	243 ATX	244 ---	245 ATX
246 ---	247 ATX	248 ATX	249 ---	250 ---
251 ATX	252 ATX	253 ATX	254 TTU	255 ATX
256 LSI	257 ATX	258 ATX	259 ---	260 ---
261 SCH	262 ATX	263 CAN	264 ICT	265 CAN
266 CSY	267 CAN	268 CAN	269 FDG	270 ---
271 ---	272 ATX	273 ---	274 MCI	275 ITT
276 ONE	277 SNT	278 ---	279 MAL	280 ADG
281 ---	282 ATX	283 MCI	284 MCI	285 ---
286 ---	287 ---	288 MCI	289 MCI	290 ---
291 ---	292 ATX	293 PRO	294 ---	295 ---
296 ---	297 ARE	298 ---	299 CYT	

321 ATX	322 ATX	323 ATX	324 HNI	325 ATX
326 UTC	327 ATX	328 ATX	329 TET	330 TET
331 ATX	332 ATX	333 MCI	334 ATX	335 SCH
336 ATX	337 FST	338 ATX	339 ---	340 ---
341 ATX	342 ATX	343 ATX	344 ATX	345 ATX
346 ATX	347 UTC	348 ATX	349 DCT	350 CSY
351 ATX	352 ATX	353 ---	354 ---	355 ---
356 ATX	357 ---	358 ATX	359 UTC	360 ---
361 CAN	362 ATX	363 CAN	364 HNI	365 MCI
366 UTC	367 ATX	368 ATX	369 TDD	370 TDD
371 ---	372 ATX	373 TDD	374 ---	375 TNO
376 ---	377 GTS	378 ---	379 ---	380 ---

the long awaited

381 ---	382 ATX	383 TDD	384 FDT	385 CAB
386 TBQ	387 CAN	388 ---	389 ---	390 ---
391 ---	392 ATX	393 EXF	394 ---	395 ---
396 ---	397 TDD	398 ---	399 ARZ	

421 ATX	422 ATX	423 ATX	424 ATX	425 TTH
426 ATX	427 ---	428 ATX	429 ---	430 ---
431 ATX	432 ATX	433 ATX	434 AGN	435 ATX
436 IDN	437 ATX	438 ATX	439 ---	440 TXN
441 ATX	442 ATX	443 ATX	444 MCI	445 ATX
446 ATX	447 ATX	448 ATX	449 ---	450 USL
451 ATX	452 ATX	453 ATX	454 ALN	455 ---
456 MCI	457 ATX	458 ATX	459 ---	460 ---
461 CAN	462 ATX	463 CAN	464 --	465 CAN
466 ALN	467 ICT	468 ATX	469 ---	470 ---
471 ALN	472 ATX	473 ---	474 ---	475 TDD
476 TDD	477 ---	478 AAM	479 ---	480 ---
481 ---	482 ATX	483 ---	484 TDD	485 TDD
486 TDX	487 ---	488 ---	489 TOM	490 ---
491 ---	492 ATX	493 ---	494 ---	495 ---
496 ---	497 ---	498 ---	499 ---	

521 ATX	522 ATX	523 ATX	524 ATX	525 ATX
526 ATX	527 ATX	528 ATX	529 MIT	530 ---
531 ATX	532 ATX	533 ATX	534 ---	535 ATX
536 ALN	537 ATX	538 ATX	539 ---	540 ---
541 ATX	542 ATX	543 ATX	544 ATX	545 ATX
546 UTC	547 ATX	548 ATX	549 ---	550 CMA
551 ATX	552 ATX	553 ATX	554 ATX	555 ATX
556 ATX	557 ALN	558 ATX	559 ---	560 ---
561 CAN	562 ATX	563 CAN	564 ---	565 CAN
566 ALN	567 CAN	568 ---	569 ---	570 ---
571 ---	572 ATX	573 ---	574 AMM	575 ---
576 ---	577 GTS	578 ---	579 LNS	580 WES
581 ---	582 ATX	583 TDD	584 TDD	585 ---
586 ATC	587 LTQ	588 ATC	589 LGT	590 ---
591 ---	592 ATX	593 TDD	594 TDD	595 ---
596 --		597 ---	598 ---	599 ---

621 ATX	622 ATX	623 ---	624 ATX	625 NLD
626 ATX	627 MCI	628 ATX	629 ---	630 ---
631 ATX	632 ATX	633 ATX	634 ATX	635 ATX
636 CQU	637 ATX	638 ATX	639 BUR	640 ---
641 ATX	642 ATX	643 ATX	644 CMA	645 ATX
646 ---	647 ATX	648 ATX	649 ---	650 ---
651 ---	652 ATX	653 ---	654 ATX	655 ---
656 ---	657 TDD	658 TDD	659 ---	660 ---
661 CAN	662 ATX	663 CAN	664 UTC	665 CAN
666 MCI	667 CAN	668 CAN	669 UTC	670 ---

800 translation table!

671 ---	672 ATX	673 TDD	674 TDD	675 ---
676 ---	677 ---	678 MCI	679 ---	680 ---
681 ---	682 ATX	683 MTD	684 ---	685 ---
686 LGT	687 NTS	688 ---	689 ---	690 ---
691 ---	692 ATX	693 ---	694 ---	695 ---
696 ---	697 ---	698 NYC	699 PLG	

720 TGN	721 ---	722 ATX	723 ---	724 RTC
725 SAN	726 UTC	727 MCI	728 TDD	729 UTC
730 ---	731 ---	732 ATX	733 UTC	734 ---
735 UTC	736 UTC	737 MEC	738 MEC	739 ---
740 ---	741 MIC	742 ATX	743 EDS	744 ---
745 ---	746 ---	747 TDD	748 TDD	749 TDD
750 ---	751 ---	752 ATX	753 ---	754 TSH
755 ---	756 ---	757 TID	758 ---	759 MCI
760 ---	761 ---	762 ATX	763 ---	764 AAM
765 ---	766 ---	767 UTC	768 SNT	769 ---
770 GCN	771 SNT	772 ATX	773 CUX	774 ---
775 ---	776 UTC	777 MCI	778 UTC	779 TDD
780 TDD	781 ---	782 ATX	783 ALN	784 ALG
785 SNH	786 *1	787 ---	788 ---	789 TMU
790 ---	791 ---	792 ATX	793 ---	794 ---
795 ---	796 ---	797 TID	798 TDD	799 --

821 ATX	822 ATX	823 THA	824 ATX	825 MCI
826 ATX	827 UTC	828 ATX	829 UTC	830 ---
831 ATX	832 ATX	833 ATX	834 ---	835 ATX
836 TDD	837 TDD	838 ---	839 VST	840 ---
841 ATX	842 ATX	843 ATX	844 LDD	845 ATX
846 ---	847 ATX	848 ATX	849 ---	850 TKC
851 ATX	852 ATX	853 ---	854 ATX	855 ATX
856 ---	857 TLS	858 ATX	859 ---	860 ---
861 ---	862 ATX	863 ALN	864 TEN	865 ---
866 ---	867 ---	868 SNT	869 UTC	870 ---
871 ---	872 ATX	873 MCI	874 ATX	875 ALN
876 MCI	877 UTC	878 ALN	879 ---	880 NAS
881 NAS	882 ATX	883 ---	884 ---	885 ATX
886 ALN	887 ETS	888 MCI	889 ---	890 ---
891 ---	892 ATX	893 ---	894 ---	895 ---
896 TXN	897 ---	898 CGI	899 TDX	

921 ---	922 ATX	923 ALN	924 ---	925 ---
926 ---	927 ---	928 CIS	929 ---	930 ---
931 ---	932 ATX	933 ---	934 ---	935 ---
936 RBW	937 MCI	938 ---	939 ---	940 TSF
941 ---	942 ATX	943 ---	944 ---	945 ---
946 ---	947 ---	948 ---	949 ---	950 MCI
951 BML	952 ATX	953 ---	954 ---	955 MCI

800 exchange translations

956 ---	957 ---	958 *2	959 *2	960 CNO
961 ---	962 ATX	963 SOC	964 ---	965 ---
966 TDX	967 ---	968 TED	969 TDX	970 ---
971 ---	972 ATX	973 ---	974 ---	975 ---
976 ---	977 ---	978 ---	979 ---	980 ---
981 ---	982 ATX	983 WUT	984 ---	985 ---
986 WUT	987 ---	988 WUT	989 TDX	990 ---
991 ---	992 ATX	993 ---	994 ---	995 ---
996 VOA	997 ---	998 ---	999 MCI	

NOTES:

*1 -- RELEASED FOR FUTURE ASSIGNMENT

*2 -- These NXX codes are generally reserved for test applications. They may be reserved for access tandem testing from an end office.
Note also: the following NXX's are dedicated for RCCP (Radio Common Carrier Paging) under the discretion of the local exchange carrier:
202, 212, 302, 312, 402, 412, 502, 512, 602, 612, 702, 712, 802, 812, 902, and 912.

OCN Reference List:

ADG - Advantage Network, Inc.
ALG - Allnet Communication Services
AAM - ALASCOM
ARZ - AmeriCall Corporation (Calif.)
ATX - AT&T
BUR - Burlington Tel.
CAN - Telcom Canada
CQU - ConQuest Comm. Corp
CUX - Compu-Tel Inc.
DCT - Direct Communications, Inc.
EDS - Electronic Data Systems Corp.
EXF - Executines of Florida, Inc.
FDN - Florida Digital Network
FST - First Data Resources
GTS - Telenet Comm. Corp.
ITT - United States Transmission Sys
LDL - Long Distance for Less
LNS - Lintel Systems
LTQ - Long Distance for Less
MCI - MCI Telecommunications Corp.
MEC - Mercury, Inc.
MIT - Midco Communications
NLD - National Data Corp.
NTS - NTS Communications
ONE - One Call Communications, Inc.
PLG - Pilgrim Telephone Co.
RBW - R-Comm

AGN - AMRIGON
AMM - Access Long Distance
ARE - American Express TRS
ATC - Action Telecom Co.
BML - Phone America
CAB - Hedges Communications
CNO - COMTEL of New Orleans
CSY - COM Systems
CYT - ClayDesta Communications
DLT - Delta Communications, Inc.
ETS - Eastern Telephone Systems, Inc.
FDG - First Digital Network
FDT - Friend Technologies
GCN - General Communications, Inc.
HNI - Houston Network, Inc.
LDD - LDDS-II, Inc.
LGT - LITEL
LSI - Long Distance Savers
MAL - MIDAMERICAN
MDE - Meade Associates
MIC - Microtel, Inc.
MTD - Metromedia Long Distance
NTK - Network Telemanagement Svcs.
ONC - OMNICALL, Inc.
PHE - Phone Mail, Inc.
PRO - PROTO-COL
RTC - RCI Corporation

and 900 translations too!

SAN - Satelco
SDY - TELVUE Corp.
SLS - Southland Systems, Inc.
SNT - SouthernNet, Inc.
TBQ - Telecable Corp.
TDX - Cable & Wireless Comm.
TEM - Telesystems, Inc.
TET - Teltec Savings Comm. Co.
THA - Touch America
TKC - TK Communications, Inc.
TMU - Tel-America, Inc.
TOM - TMC of Montgomery
TSF - SOUTH-TEL
TTH - Tele Tech, Inc.
TXN - Tex-Net
UTC - U.S. Telcom, Inc. (U.S. Sprint)
VST - STAR-LINE
WUT - Western Union Telegraph Co.
SCH - Schneider Communications
SIR - Southern Interexchange Services
SNH - Sunshine Telephone Co.
SOC - State of California
TDD - Teleconnect
TED - TeleDial America
TEN - Telesphere Network, Inc.
TGN - Telemanagement Consult't Corp.
TID - TMC South Central Indiana
TLS - TELE-SAV
TNO - ATC Cignal Communications
TOR - TMC of Orlando
TSH - Tel-Share
TTU - Total-Tel USA
USL - U.S. Link Long Distance
VOA - Valu-Line
WES - Westel

NOTE: Where local telcos, such as Illinois Bell offer 800 service, they purchase blocks of numbers from AT&T on prefixes assigned to AT&T. They are free to purchase blocks of numbers from any carrier of their choice however.

900 Series Prefix to OCN translation table

Please note that this differs from the 800 table, because much fewer of the 900 NXXs are assigned.

200 ATX	202 AME	210 ATX	220 ATX	221 TDX
222 ONC	223 TDX	225 PAC	226 MCI	233 TDX
234 TEN	240 USW	248 AME	250 ATX	258 TEN
254 TTU	255 SNT	260 ATX	264 ADG	266 CSY
272 BLA	273 CAN	275 ITT	280 AME	282 LGT
283 PAC	288 GNW	297 CAN	300 ATX	301 AME
302 AME	303 PAC	321 TEN	322 TDX	327 ETS
328 ATX	331 TET	332 PLG	333 USW	335 BLA
342 ATX	344 ATX	345 ALN	346 UTE	350 ATX
364 GNW	366 ONC	369 TEN	370 ATX	377 GTS
386 UTE	388 SNT	399 ARZ	400 ATX	407 ATX
410 ATX	420 ATX	422 ALN	426 PLG	428 AME
430 USW	444 ONC	445 PHE	446 MCI	450 AME
451 CAN	456 TEN	463 UTE	478 AAM	479 ARZ
480 ATX	483 GMW	488 ONC	490 USW	500 ATX
505 PAC	520 ATX	529 MIT	536 BUR	540 ALN
543 ALN	545 GCA	550 ALN	555 ATX	567 ALN
580 USW	590 ATX	595 CAN	600 ATX	620 AME

900 translations &

624 PAC 626 CSY 628 AME 630 CAN 633 MIT
639 PLG 643 CAN 645 CAN 650 ATX 654 TEN
656 SNT 660 ATX 661 UTE 663 MDE 665 ALN
666 ONC 670 CAN 677 CAN 678 MCI 680 ATX
686 LTG 690 CAN 698 NYT 699 PLG 701 BLA
710 TGN 720 ATX 722 PAC 724 RTC 725 SNT
727 GCA 730 ATX 739 CSY 740 ATX 741 TEN
746 ITT 750 CAN 753 ALN 765 ALN 773 ATX
777 PAC 778 AME 780 AME 786 ATX 790 CAN
792 CAN 801 BLA 820 ATX 830 CAN 843 PAC
844 PAC 847 UTE 850 ATX 860 ATX 866 AAM
870 CAN 872 TEN 887 ETS 888 CIS 900 TDX
901 BLA 903 ATX 909 ATX 924 AME 932 ATX
948 ARZ 949 MIC 963 TEN 970 MIC 971 MIC
972 MIC 973 MIC 974 ALN 975 ALN 976 ATX
988 MCI 990 MCI 991 ALG 993 SNT 999 TEN

With 900 service, you pay more for the information than for the transport of the call. This varies typically from 35 cents to a few dollars for either a timed service, or a "as long as you like" duration-sensitive service. There are two sub-species of 900 service, AT&T and "everybody else".

Everybody else is handled exactly as 800 service above, except the IEC will probably use the ANI information to send you a bill. (Either directly, or through your BOC, each situation is governed by applicable tariffs and contractual arrangements between the IEC and the BOC.)

AT&T 900 is a curious monster indeed. It was designed as a "mass termination" service. When you dial a 900 number by AT&T (such as the "hear space shuttle mission audio" number) you get routed to one of twelve "nodes" strewn throughout the country. These nodes are each capable of terminating 9,000 calls *per second*. There are several options available, where the customer and/or the IP pay for all/part of the call. The big difference between 800 and AT&T 900 is *not* "who pays for the call" (there are free 900 numbers) but "how many people can it handle at once". The IP is responsible for providing program audio. AT&T is prohibited from providing audio-program services (i.e., tape recorded messages). As with any rule, there are exceptions to these as well.

Additional OCN's:

AME - Ameritech
BLA - Bell Atlantic
GCA - GTE California
GMW - GTE Midwest
GNW - GTE Northwest
NYT - New York Telephone
PAC - Pac Bell
USW - U.S. West
UTE - United Tel

Glossary:

ANI - Automatic Number Identification. An MF sequence that identifies your line for toll billing information. Often confused with ANAC (Automatic Number Announcement Circuit)

glossary of terms

which reads your number back in a synthesized voice.

BOC - Bell Operating Company. An often misused term that in general usage means "your local exchange carrier." Since most of the telephones in the country are served by what used to be the Bell system, we tend to use the term. The proper term in this case, however IS "Exchange Carrier [EC]". They provide service within your LATA.

FG-A - Feature Group A. Line Side termination for Long Distance carriers. The old 555-1234 for Widget Telephone Company, then dial an access code, and the number style dialing is called FG-A.

FG-B - Feature Group B. Trunk Side termination for Long Distance carriers. 950 service. This is LATA wide service, and doesn't cost the customer message units. ANI is only provided when the trunks terminate in the End Office (as opposed to an access tandem).

FG-D - Feature Group D. Trunk Side termination. Provides 10xxx dialing, 1+ pre-subscription dialing, and Equal Access 800/900 service. Only available in electronic offices and some 5XB offices (through a beastie called an Adjunct Frame.)

GAB - Group Audio Bridging. Where several people call the same number, to talk to other people calling the same number. "Party" or "Chat" lines.

IEC - Inter-Exchange Carrier. Someone who actually carries calls from place to place. AT&T, Sprint, MCI are all IECs.

IP - Information Provider. Someone who sells a value-added service over the telephone. Where you pay for the *information* you're receiving, as well as the cost of *transport* of the call.

NXX - Notation convention for what used to be called a "prefix". N represents the digits 2 through 9, and X represents the digits 0 through 9. There are 800 valid NXX combinations, but some are reserved for local use. (411 for Directory, 611 for Repair Bureau, 911 for emergency, etc.)

ONI - Operator Number Identification. In areas with some styles of party-line service, the CO cannot tell who you are, and the operator will come on and say, "What number are you calling from?". You can lie, they have to trust you. They *may* know which *prefix* you're coming from, though.

PTN - Plant Test Number. A regular 10 digit number assigned with your inward WATS line. This may NOT be a "dialable" number from the local CO. (A friend has a WATS line in Amherst, MA [413-549, #5 ESS] and you cannot dial the PTN locally, but you can if you come in on a toll trunk.)

SAC - Special Area Code. Bellcore speak for area codes that aren't really places, but classes of service.

HACKERS

(continued from page 3)

California group of computer enthusiasts, the Roscoe Gang, who met in a pizza parlor in the Los Angeles area. The group also stayed in contact through a variety of computer bulletin board systems, including one, 8BBS Santa Clara, California, run by employees of Digital.

In 1981 Mr. Mitnick and three other group members were arrested on charges of stealing technical manuals from the Pacific Telephone Company. Mr. Mitnick was convicted and served six months in a youth detention center.

He was caught again by University of Southern California officials in 1983 trying to break into the school's computers. In another incident, Mr. Mitnick fled to Israel to avoid prosecution after being accused of tampering with a computer storing credit information at TRW.

In December 1987 he was convicted of stealing software from Microport Systems in Santa Cruz, and was sentenced to 36 months of probation.

What made Mitnick "the best", according to a friend, was his ability to talk people into giving him privileged information. He would call an official with a company he wanted to penetrate and say he was in the maintenance department and needed a computer password. He was so convincing that they would give him the necessary names or numbers.

Mr. Mitnick was supposedly able to avoid being apprehended by tampering with telephone company switching equipment to mask his location. An internal memo of the Pacific Telephone Company indicated that Mitnick had compromised all of that company's switching systems.

Investigators believe that Mitnick may have been the instigator of a false report released by a news service in April 1988 that Security Pacific National Bank lost $400 million in the first quarter of 1988. The report, which was released to the NY Stock Exchange and other wire services, was distributed four days after Mitnick had been turned down for a job at Security Pacific.

The false information could have caused huge losses for the bank had it reached investors, but the hoax was uncovered before that could happen.

The prosecutor said Mitnick also penetrated an NSA computer and obtained telephone billing data for the agency and several of its employees.

As of this writing, Mitnick has been sentenced to a year in jail. They won't even let him use the phone, out of fear of what he might do.

* * *

Story Number Two: An 18-year-old telephone phreak from Chicago who electronically broke into U.S. military computers and AT&T computers and copied 55 programs was

IN JAIL

sentenced to nine months in prison on Tuesday, February 14 in Federal District Court.

Herbert Zinn, Jr. was found guilty of violating the Computer Fraud and Abuse Act of 1986 by Judge Paul E. Plunkett. In addition to a prison term, Zinn must pay a $10,000 fine and serve two and a half years of federal probation when released from prison.

United States Attorney Anton R. Valukas said, "The Zinn case will serve to demonstrate the direction we are going to go with these cases in the future. Our intention is to prosecute aggressively. What we undertook is to address the problem of unauthorized computer intrusion, an all-too-common problem that is difficult to uncover and difficult to prosecute...."

Zinn, a dropout from Mather High School in Chicago, was 16 at the time he committed the intrusions, using his home computer and modem. Using the handle "Shadow Hawk", Zinn broke into a Bell Labs computer in Naperville, Illinois, an AT&T computer in Burlington, North Carolina, and an AT&T computer at Robbins Air Force Base in Georgia. No classified material was obtained, but the government views as "highly sensitive" the programs copied from a computer used by NATO which is tied into the U.S. missile command. In addition, Zinn gained access to a computer at an IBM facility in Rye, New York and logged into computers of Illinois Bell Telephone Company and the Rochester Telephone Company.

Assistant United States Attorney William Cook said that Zinn obtained access to the AT&T/Illinois Bell computers from computer bulletin board systems, which he described as "...just high-tech street gangs". During his bench trial in January, Zinn spoke in his own defense, saying that he copied the programs to educate himself, and not to sell them or share them with other phreaks. The programs copied included very complex software relating to computer design and artificial intelligence. Also copied was software used by the BOC's (Bell Operating Companies) for billing and accounting on long distance telephone calls.

The authorities didn't find it difficult to identify Zinn. But rather than move immediately, they decided to give him enough time to make their case stronger. For over two months, all calls from his telephone were carefully audited. His activities on computers throughout the United States were noted, and logs were kept. Security representatives from Sprint made available notes from their investigation of his calls on their network. Finally, the "big day" arrived, and the Zinn residence was raided by FBI agents, AT&T security representatives, and Chicago police detectives. At the time of the raid, three computers, various modems,

and other computer peripheral devices were confiscated.

As of this writing, Zinn is still in jail.

* * *

Conclusions: This is without a doubt one of the most disturbing articles we've printed since we began publishing in 1984. When people actually start winding up in jail because of playing with computers, it's time to start asking some very serious questions.

Let's start with the Mitnick story. Here we have what appears to be a malicious person who is determined to get those who have crossed him. OK, not very nice. In fact, this could well be a nasty, vindictive human being. And we've already proven that he has a history of trouble with the law. But is this enough to lock him up without bail?

In regular life in almost any democratic society, the answer would be a resounding no. But there are special circumstances here: computers. Doing nasty things with computers has become infinitely worse than doing nasty things without computers. That's why a murderer would get bail so much easier than Kevin Mitnick. Because of computers.

So let's try and pretend that computers don't really exist. Where does that leave us? He would have to have disconnected Kristy McNichol's phone using wire clippers. Vandalism, maybe trespassing. That's good for a fine of maybe $100.

He and a friend walked into the North American Air Defense Command Center one day. They didn't break anything and they soon left. Had they been caught, they would have been thrown off the grounds, maybe arrested for trespassing and held overnight. The person who left the door open would be fired.

Mitnick managed to manipulate central office switches by walking through their doors and adjusting them. Nobody questioned him or tried to stop him. He called up a news service and told them a fake story about a bank which they almost printed. Again, nobody questioned him.

In our society, such a person would be classified as a mischief maker, at worst a real pain in the ass. Such people currently exist all over the place. But because Mitnick used computers to perform his mischief, he's another John Hinckley.

Society is indeed endangered by what's happening here. But Mitnick has nothing at all to do with it. He is simply demonstrating how vulnerable our information and our way of life has become. If one person can cause such chaos, then clearly the system is falling apart at the seams.

The Zinn case is equally deplorable. A bright kid is languishing in prison because he didn't know when to stop exploring. The authorities admit they did nothing

to stop him so that he would get himself in deeper. What would have been wrong with a simple warning? It might have been enough to stop him from logging into any more systems. There would have been no trial and an intelligent 18-year-old would not be locked away.

All of the papers accused Zinn of stealing software. But nothing was taken. All he did was *copy* some programs. If these programs were so valuable, why in hell was he able to download them over the phone lines? To even suggest that this is the same as stealing is a gross distortion. There is not one shred of evidence that this kid meant to sell these programs or benefit in any way except his own knowledge. This isn't surprising -- most hackers are primarily interested in learning.

But they say a message had to be sent to stop this kind of thing from happening. The message here is that our nation's brightest kids are being imprisoned for being a little too inquisitive. And that's a frightening thought.

Judges should consider what actually took place and forget about the fact that computers were involved. Would it even be a crime if computers weren't involved? And what about intent? Did the person willfully do something that could be detrimental to an organization? Or was that simply a side-effect of the organization's carelessness?

Much can be learned from what the hackers uncover. While hackers are far from being knights in shining armor, the notion of their being criminals is so far from the truth that it's almost funny. These are kids doing what kids have done for all time. The only difference here is that they've learned how to use a tool that the rest of us have ignored. And unless more of us know how to use this tool, there will be many more abuses. Not just abuses *of* the tool. Abuses *by* the tool. That's where the real danger is.

We take a very hard line on this. Hacking is not wrong. Hacking is healthy. Hacking is *not* the same as stealing. Hacking uncovers design flaws and security deficiencies. Above all else, hacking proves that the ingenuity of a single mind is still the most powerful tool of all.

We are hackers. We always will be. Our spirits will not be crushed by these horrible happenings. Call us co-conspirators, fellow anarchists, whatever you want. We intend to keep learning. To suppress this desire is contrary to everything that is human.

Like the authors who rose to defend Salman Rushdie from the long arm of hysteria, we must rise to defend those endangered by the hacker witchhunts. After all, they can't lock us all up. And unless they do, hacking is here to stay.

Wargames Dialer

Dear 2600:

In your Spring 1988 issue (Volume 5, Number 1), you had a listing for the "Wargames Dialer Program". What computer was this written for? I own an Apple //c, and it will work for it, if you change line 30 from:

```
30 PRINT Q$ "    " N$
      to
30 PRINT "ATDT "N$
```

I don't know what modem type you wrote it for, but the change will fix it to operate on a Hayes compatible modem. Thanks alot for the great mag!

Phloyd Scaari
Somewhere in the Underground

More ANI's

Dear 2600:

The ANI for 817 (Fort Worth, Texas) is 211. Now, how about a list of ringback numbers?

RR

Dear 2600:

ANI is 511 in area code 716. The ANI for 602 is 593-5010.

Dear 2600:

The ANI for the 509 area is 560, then enter 1 until the computer comes on. The ringback is 571 plus the last four digits of the phone number, hang up, pick it up again (you should hear a tone) then hang up again. 590 from a payphone leaves the phone "off hook".

Radio Shack sells this nifty little device that lets you forward your calls to another number. I have found that you can call a number, leave it unprogrammed, and then you will get a dial tone. It is battery operated and AC operated. This is great for beige boxing at home.

KH

Blue Box Questions

Dear 2600:

Since taking control of trunks via blue boxing thru long distance companies is nearly common knowledge, I ask you this question:

Why, even when a trunk is secured, is it very difficult to patch a call through?

It seems as if certain trunkable prefixes are all only local calls and outside calls to different area codes and prefixes are impossible.

Also, what do the squares that contain different symbols on the front cover mean?

Santa Claus
Santa's Workshop, N.P.

Things are just not the same as they were years ago. It is possible to seize a trunk and still not be able to accomplish

much, depending on what kind of restrictions are enabled by the company involved.

The little squares on the front cover are exactly what they appear to be. Shocked?

Dear 2600:

I enjoyed blue boxing in my home town for about two years until November 7, 1987. Suddenly the 2600 hertz tone would not break the 800 line anymore, so I assume that we switched to ESS, although another exchange in my home town is still "blue-boxable". Is there *any* way around this? Perhaps calling from an ESS to a crossbar exchange and then boxing?

Is my blue box *totally useless* in my exchange now? Should I throw it out the window and resort to those dangerous access codes?

Could you please tell me any other ways of obtaining a *free* phone call under ESS conditions (besides using someone else's access code and red boxing)?

I was used to calling BBS's for hours at a time. Now I can't even do that due to the rates of long distance! Could you please print some uses of blue boxes under ESS and other ways for phone phreaks to obtain service?

You always print ways to hack other computers and print numbers of far-away BBS's, but for us guys that do *not* live in large metropolitan cities, this is useless to us IF we have to pay for the call! Your magazine has a heavy interest on computers, but why can't you print more on phreaking instead of hacking? After all, your magazine is named 2600! Not Unix V3.0!

Boxed In TX

Blue boxes can still work from an ESS line, although it is generally a bit more dangerous. We suspect the change took place somewhere between your exchange and the 800 number.

While blue boxing is a great way to explore the phone system, you should know that it's extremely dangerous, especially from your home phone. Access codes are also dangerous to use from your home phone or from any phone for an extended period. Red boxing (sending coin tones from a payphone) is probably safer since it's hard for the phone company to know that those aren't real quarters it's hearing. But if a particular phone has been abused a lot, you could have problems if you continue to red box from it.

Your troubles are not unique. But there are always ways around the system. Keep experimenting and you'll most certainly find one.

A Scary Tale

Dear 2600:

Let this be a warning to those who engage in illegal activity.

On June 27, 1988, I came home from being out with friends at 1:45 in the morning. I parked my car in front of my apartment and got out. I am normally a very security minded person, always looking over my shoulder, never getting overconfident with my sense of security. Many people know me in the IBM/Apple modem/hacking world, but I never let people know me too well.

Or so I thought.

As I stepped up my walkway to my building, I heard someone call my name. Before I turned around, I knew something was wrong. FBI agents as well as state police and local detectives had been watching and waiting for me all day. In no time there were police cars everywhere, and I was shoved up against a car and searched and handcuffed, the whole neighborhood ablaze with flashing lights.

Of course I didn't say anything. Of course they played games like "Let's just go inside and talk this all over." I have always known better than to keep anything in my apartment that could incriminate me, but why attempt to make their job any easier?

Well, that was six months ago. I am still in jail.

That night I was driven 250 miles to a small, conservative farm town, a place I had never been to in my life. At my arraignment three days later, I found out that I was being charged with six counts of computer fraud-related charges, and my bond is a hefty $150,000, cash only. My parents live in another part of the country, and I have few connections with them anymore, and unlike your average juvenile, I can't call mummy and daddy up and expect them to come running, cash in hand.

Now I can handle having to serve time for my own mistakes, but the way I was caught will show you that everybody who does anything illegal better be careful.

In February, 1988, I met with a person who I had known through various bulletin boards. I was going to school in the state he was from, so we decided to meet each other.

I drove and met him, ate din-

ner, and talked. He and I got along quite well, but at no point did he ever know my "real" name. Of course in the "modem community", relationships like that are common and understood.

That was the last time I saw him.

About a month later, this friend was visited by state police as well as security people from Sprint. Apparently another "hacker" (I'm using that term loosely) had an argument with said friend, and as a type of revenge, called Sprint Security and reported that said friend was a habitual code abuser. It took very little time for security people from Sprint and his local telco to put a DNR-type register on his two step-by-step phone lines.

Two months and 30 rolls of DNR paper later, a search warrant was obtained. His residence (he is a juvenile) was searched, and all computer and telephone equipment was taken and brought to a state police post for examination. At this time, said friend was smart enough to not talk without a lawyer present, so the police left, leaving him with his parents, no charges pending at that time.

He was smart to keep quiet. Too bad this trend did not continue.

Many people underestimate police investigators or the FBI. Don't ever let yourself be part of that group.

My friend was questioned several times after that. I now have all transcripts of all conversations. He told various names of people all over the country who had supplied him with codes, passwords, accounts, etc. He also said that he had a friend who was currently living in the state, who was involved with various activities similar to his own. He told the police what he knew of me, which wasn't too much, as well as what he thought my first and last name was.

Some time later, the police returned and asked him if he had any more information, as they had been able to find nothing on this other person he had mentioned. He could think of little else, except that he thought I had lived in a particular place prior to my living in his state.

The police wrote to that place and state, giving a basic age and description, and asked for copies of any mug shots they might have fitting that description.

Many years ago, some friends and I were arrested for trying to purchase alcohol

underage. Although the charges were dropped, that picture stayed on file.

The police came back to this individual and presented several dozen photographs of the people who had fit that description.

The police report says that he "without hesitation pointed out photograph #13 as being the individual he knew."

The next day, warrants were issued, and today, here I am in a county jail.

Since that time, I have said absolutely nothing. I did not talk to anyone and try to lie, or offer to turn anyone else in. I simply refused to talk to anybody for any reason. I had to front $5,000 to a lawyer, and because I have not said anything or made any statement, I may be able to walk away from this, uncharged.

But, the damage is done. I was in my final year of college and taking summer courses. I had an excellent job with a well known DoD contractor, and my future looked good. I was no longer doing anything illegal, and was keeping quite straight.

All of that is gone now. Even if I come out of this without charges, I have lost an entire semester of school, and have little hope of getting that job back after the FBI came and went through my office. I have lost six months of my life that can never be replaced.

My arrest made every paper in the state, so of course my future in this state looks bleak.

The juvenile is facing possible probation.

My message in this is that if you engage in illegal activities, you must trust nobody. There is not one person you can trust. When more than one person is caught, courts usually offer "plea bargains" or less time to those willing to testify against their friends. I cannot hold a grudge against the person that put me in here. I'd be lying if I said I never did anything wrong, but you can bet that 99 percent of the time, it will be somebody else that gets attention put on you, not yourself. It is terrible that we now live in an age where our friends today are testifying against us tomorrow.

If you ever find yourself in a similar situation, I can never stress to you how important it is to not say anything, not make any type of statement. The police are *not* here to help you. Do not try to lie or mislead them. They have more resources available than you may think. I hear people say how they would know "exactly what to say and do" if ever

arrested, but sadly enough, when leaned on, it is amazing how many people will "break". The police are good at what they do. They know how to scare you. They have told me several times that I am looking at 36 years.

The best and only thing you can do for yourself at that point is to hire a lawyer. They can find out exactly what the police have on you, and what your real position is. If the juvenile had listened to me earlier, neither of us would be in this situation. I only hope I can reach those out there that he has told on before they find themselves in a similar situation.

Every time you leave your phone number on a bulletin board, you expose yourself. You trust that the sysop will not reveal that information to anyone. Frankly, you are risking your freedom every time.

In today's "hacker world", people are going to have to better secure themselves if they want to avoid a situation similar to the one I am in.

Wish me luck.

The Disk Jockey

Your letter provides a great deal of sobering insight. We hope this is not wasted on our readers.

While we don't know what, if anything, you did, it sure doesn't sound as if you are being treated fairly. You imply that you've been sitting in jail for six months without being charged with anything. If this is true, get rid of your lawyer and go back to those same newspapers that reported what happened. Go public and get some people behind you.

Naturally, if you feel this may backfire and encourage the authorities to file charges, don't do it. Once you're out, however, let the truth be known. If you think the system is screwing you, speaking out about it may prevent the same thing from happening to others.

If this is nothing more than a case of fraudulent phone calls, sitting in jail for six months is preposterous. Even credit card fraud, which to us is nothing less than stealing, should be dealt with by making the offender compensate the victim for their losses. Apparently, though, not everyone holds this view.

We have some difficulty understanding why you're not answering any questions. If you don't know any names or details, you really can't put the finger on anyone. If you do know names and you're protecting them, then you are indeed being quite noble. But

(continued on page 46)

HOW PAYPHONES

by The Infidel

Fortress phones, a.k.a. payphones, are something that every phreak should have had experience with at least once in their career. Such devices as the red box and the green box also make the fortress a great place to phreak from. In this article, I will try to explain how a payphone works, and how one can (ab)use it.

Basically, payphones are not too different from normal phones, requiring all the speech and signaling facilities of ordinary telephones, but, in addition, requiring signals to handle the charge for the call with the money inserted. However, the payphone itself has undergone some changes through the years.

Some Payphone History

In most coin telephones, the stations operate on a pre-pay basis, that is, the coins must be deposited before the call can be completed. A few of the older central offices using step-by-step equipment that had only a few public telephones accepted deposits after completion of the call. This form of operation, post-pay coin service, was chosen usually because of the long distance between the local community dial office and the serving toll switchboard, which often resulted in large costs due to the returning of coins on uncompleted calls.

The older versions of pre-payphones (the ones made famous by David in War Games), the A-type set, would produce a dialtone only *after* a coin was deposited. These were also rotary phones. As ESS emerged, with such options as 911 and 411 directory assistance, the need for a dialtone-first phone emerged, the C-type station, which resulted in the dialtone-first rotary phone.

With the advent of touch tone, calling cards, and long-distance carriers, payphones developed into the touch tone, dialtone-first public telephone. As you may have noticed, the intermediate telephone, the rotary, dialtone-first phone is very hard to come by these days, obviously due to the increasing demand in the many services now offered by Ma Bell and other companies which take advantage of the touch tone service.

Up until 1978, signalling for coin deposits was accomplished by a single-frequency tone, sent in pulses, as they are today. As an Automated Coin Toll Service (ACTS) appeared necessary, to automate the routine functions of TSPS (Traffic Service Position System) Operators, there developed a need for improvements in the station to prevent simulation of the coin signals, and therefore, toll fraud. As a result, before the introduction of TSPS/ACTS, all coin sets manufactured after 1977 were then equipped with dual-frequency oscillators. These coin boxes

produced the current form of coin signalling, the dual-frequency tone. This resulted in the D-type station, which, due to its power requirements and electronic components, rather than mechanical, could only be used in a dialtone-first environment, and is, therefore, what we see today.

Operation Logic

As noted above, the payphone is, essentially, the same as a customer-owned telephone, with the main difference being, quite obviously, the presence of the coin box.

In the design of the coin box, the following must be considered. The coin box can be very sophisticated, to handle many functions, thus requiring a very simple exchange to just receive all billing information from the phone itself. Or, vice versa, the coin box can be quite simple, and the exchange can be much more complex, to interpret the data from the box needed to place the call and charge a toll for it.

Today's standard Western Electric/AT&T telephone follows the latter, a more simple coin box design. These boxes, signal forward to the exchange the value of each coin inserted, using tone pulses. This technique requires Coin and Fee Check (C and FC) equipment in the exchange, ACTS, to carry out the call accounting necessary between the value of the coins inserted and the rate of charging of the call. This arrangement lets you insert coins into the phone at any time during the call, but its main disadvantage is that the speech transmission must be interrupted while the coin value is signalled to the exchange.

Thus, the property of requesting a coin for a call *is not in the phone*, but in the exchange itself. If you were to take a payphone home with you and hook it up to your line, it would not request a coin deposit. On the other hand, if you were to tap into a payphone line and tried to place a call, you would get the familiar coin deposit request message.

"Owning a payphone, especially in high traffic areas, can be quite advantageous."

What Happens To Your Money?

When you first put your coin in the slot, it is tested for size, weight and material. Size is determined by the size of the slot the coin passes through, as well as the coin chute it slides through in the phone itself. A coin that is too large is not allowed into the phone itself, while one too small just falls through without having accomplished anything. Material is identi-

fied by the use of magnetic fields; slugs will be deflected, while coins will not. If the coin is right, it is allowed to hit a sprocket, which when hit by the coin, spins a certain amount of times, determined by its weight. This spinning of the sprocket controls a tone generator within the telephone, which creates the coin deposit tones, which, in turn, the exchange then interprets to determine the amount to credit the customer.

As the payphone can accept only three different coins, there are three coin signals to identify each one. The signal consists of 1700 Hz and 2200 Hz tones generated together to produce a dual-frequency tone. The dual tone is more efficient, because it cannot be confused with (or simulated by) human speech, since the human voice can only produce one tone at a time, and is also more difficult to simulate electronically, in an effort to prevent fraud. To identify the value of the coin, the tone is sent to the exchange in pulses.

Nickel Tone: One 60 millisecond pulse (1700 Hz + 2200 Hz)

Dime Tone: Two 60 millisecond pulses separated by 60 milliseconds (1700 Hz + 2200 Hz)

Quarter Tone: Five 35 millisecond pulses separated by 35 milliseconds (1700 Hz + 2200 Hz)

As mentioned earlier, the main problem with this design is that the conversation is interrupted by the insertion of coins, which can be quite annoying on long-distance calls placed on peak hours, when the rates are highest. Yet, since the tones do interrupt the speech transmission, a phreak can send, along with the speech transmission, these same tones, generated artificially by a device known as the red box.

After the coins have been accounted for, they are held in a hopper, which is controlled by a single-coil relay. This relay is controlled by the application of negative or positive DC voltage, depending on whether the coins are to be returned or collected. The line reversal can occur by one of two ways. One way the line reversal can be accomplished is at the phone itself, via the switchhook. In the on-hook position, the

STAFF
(formerly STAFFBOX)

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch
Tish Valter Koch

Writers: Eric Corley, John Drake, Mr. French, The Glitch, Chester Holmes, The Infidel, Red Knight, Bill from RNOC, David Ruderman, Lou Scannon, Mike Yuhas, and the growing anonymous bunch.

FORTRESS PHONES

hopper will not allow coins to fall through, and so, they must be released by lifting the handset to cause a line reversal and activate the relay. The second way in which a line reversal can occur is by remote, from ACTS. ACTS can signal the station to either collect or return the coins. The signals are also in the form of dual-frequency tone bursts. Three signals ACTS can send to the fortress are the Coin Collect, Coin Return, and Ringback. These tones are also known as green box tones. The frequencies of these tones are as follows:

Coin Collect: 700 Hz + 1100 Hz (900ms)

Coin Return: 1100 Hz + 1700 Hz (900ms)

Ringback: 700 Hz + 1700 Hz (900ms)

The function of the first two should be obvious, but the Ringback may be unclear. When you walk away from a phone after not having deposited money for overtime, the phone rings. That's ACTS. It's not actually "calling" the payphone, but sending a signal to the station to order it to ring. When you pick up the phone and hear the message, "Please deposit 40 cents," that's also ACTS playing the recording. After you hang up again or don't deposit your change, ACTS signals a TSPS operator, who then breaks in and asks for the money personally, since Telco knows you're definitely not going to put money in a phone just because a machine asks you to. If you've been coerced into handing over your money, it's also ACTS which then thanks you.

Alternate Designs

An alternate telephone design allows for a drastically less complex exchange, while requiring a much more sophisticated coin box.

A payphone equipped with a "pay at any time" box allows for meter pulse signals to be sent from the exchange to the payphone, with the coin box performing the call accounting. The meter pulses may be signals at 50 Hz, or tones of 12 kHz or 16 kHz, depending on the network. Therefore, the insertion of coins will not interfere with the conversation. Coins inserted prior to the call being established, and during the call, are held suspended until the control logic within the payphone (rather than the exchange) determines that they need to be collected. Coins remaining in suspension are returned to the user when the payphone goes on-hook. When no more coins are held in credit and the next meter pulse is received, the payphone requests coin insertion and then clears the call after the designated grace period has elapsed. If only part of the value of the credit held in suspension needs to be collected when the phone goes on-hook, the remainder will be lost, unless the phone is equipped with a "follow on call"

button to credit the unused portion to a call made immediately afterwards. This design, seen in England, is somewhat similar to the privately owned payphones available here.

Since the local telephone network will only allow their payphones to be connected to their special ACTS lines, privately owned payphones cannot use the ACTS to perform call accounting for it. Thus, these phones must be installed on a normal subscriber's line, a drastically less complex exchange, and, as a result, such phones require a much more sophisticated coin box.

Owning a payphone, especially in high-traffic areas, can be quite advantageous, since the owner keeps all coins collected, but only in the long run, because he has to pay for the line fee as well as the charge for the call placed. Yet, at 25 cents a call, and the current peak rate being 10.2 cents, the profits can be worthwhile. This profit is, however, substantially diminished by the expensive price tag of these units, costing between $2000 and $2500 each.

There are essentially two types of payphones out that can be purchased. One type is basically a Western Electric/AT&T look-alike. The other is the newer and fancier electronic payphone, complete with LCD digital display. Such phones offer sophisticated features such as LCD display of number being dialed, amount of money on credit, time allowed for credit, and time elapsed. Both of these telephones cost somewhere in the range of $2500-$3500, depending on the manufacturer and dealer.

"The main advantage of the payphone, to the phreak, is that it provides anonymity."

Though they appear quite different, these phones do not differ as much internally.

Both units require billing equipment within the unit itself, since normal customer lines cannot aid the phone in that capacity. As a result, these phones contain a "Rating Module", which includes a database with all inter-LATA rates and site-specific rates, as well as a clock, to determine when to apply off-peak discount rates. As rates change over time, the module can be upgraded or replaced to accommodate them, making these units quite flexible in that respect.

These telephones must also be able to discriminate between slugs and the different denominations of coins, which they do in a manner very similar to the standard payphones.

The main difference between

the two types of privately owned payphones is the manner in which each places the call.

On the Telco copies, the billing equipment within the unit receives the number to be dialed from the keypad, compares that number to the number of the line on which it is installed (pre-programmed by the owner/installer), requests the appropriate fee from the caller and then places the call itself; the keypad does not generate the actual touch tones which place the call.

The majority of the digital models, however, place calls through a PBX, often owned by ITT, and the owner, in turn, pays the company for the calls made and keeps the remaining dividends. The fact that these units utilize PBX's is not a condition required by the unit, but rather the choice of the manufacturer, seeking increased profits by the use of their own lines to place the calls for which they can then charge a fee.

When you make a call with this telephone, the number you enter with the keypad is shown on the LCD display and is then processed by the billing equipment. After requesting the corresponding fee, the call is placed through the PBX. This results in the rapid sequence of touch tones heard when placing a call with this phone. What the phone does is dial the PBX and then enter an access code used solely by the payphones. That way, the local network will not bill the owner of the phone for those calls, since the calls are being placed through the PBX, and the PBX has a toll-free dialup.

However, there are many disadvantages to this setup. Most notably, a local network operator cannot be reached through this arrangement. If you dial '0', the operator will be one selected by the company that owns the PBX used by the telephone. These operators are much more limited than the local network TSPS operators. They cannot perform such tasks as collect call placement, third party billing of calls, calling card calls, customer identification for person-to-person calls, and busy line verification. Another problem is that calling card calls cannot be made from these phones. This is due to the fact that ACCS (Automated Calling Card Service) and ACTS, which automate basic TSPS functions, are not available from within the PBX, and even if they were, the touch tones needed to enter the card number cannot be generated directly from the keypad. This lack of touch tone access also prohibits calls through other long-distance carriers via the 950 exchange. Directory assistance is also inaccessible and 911 calls cannot be placed. Many bugs in the design can also make the phone inoperable or make it enter a "Maintenance Mode" just by hitting it hard enough, since many of

(continued on page 42)

Ripoffs & Scams

In response to a massive amount of complaints, the FCC has set new guidelines for five AOS companies. These guidelines say nothing at all about rates, but they do insist that the companies allow the customer access to other long distance companies. When AOS operators handle the customer's calls, the customer must be told and he must be provided with rate information if he requests it. What they are doing is assuming that if customers are given a choice, they won't choose to be ripped off by the AOS company. It makes sense on paper, but one has to wonder what these con artists are thinking up to get around the newest stumbling blocks.

The five telephone companies are: Telesphere Network Inc. of Oakbrook Terrace, IL (the ones that run some of the ripoff 900 services as well); National Telephone Services Inc. of Rockville, MD (our old friends); Central Corporation of Fort Lauderdale, FL; Payline Systems Inc. of Portland, OR; and International Telecharge Inc. of Dallas, TX. While these are five of the biggest AOS companies (consumer groups had wanted the FCC to shut them down entirely), there are more than 200 others that are unaffected by the guidelines.

As mentioned in our Winter 1988-89 issue, MCI has been a player in this dishonest game, routing some of its zero plus calls to National Telephone Services (NTS). We received calls, letters, and e-mail from around the country telling us that this practice was working all over. Strangely enough, as of early March, we can no longer get zero plus calls to go through via MCI. While this is not exactly the public statement we had in mind, it could be a positive step if the whole country follows suit.

Speaking of NTS, our bill came recently. We had experimented with "zero plus" calls when we found out that they were being routed through an AOS. We were billed over four dollars for a collect call to ourselves, in which the word "NO" was stated emphatically. We also were billed over three dollars for calls that we hung up on after hearing the first ring. Sputtering with rage, we called NTS's unlisted 800 number (800-288-0606). (Their listed number (800-999-0687), which comes up as "National Telephone West

Coast Regional Service", is conveniently provided by none other than MCI. How convenient.) It took a very long time to get through, but when we did, the person there promised us credit without any hassle. Apparently, angry people make such companies blink.

Angry people also seem to have had an effect on Hyatt Hotels. They got tired of listening to complaints from guests about the outrageous cost of phone calls made through the AOS company that had been serving the entire chain. They were dumped in favor of AT&T. According to Gordon Kerr, vice president for management information systems at Hyatt's corporate offices, "The reality is that the service was only of acceptable to poor quality, there were oftentimes delays in putting calls through, and the charges were, frankly, outrageous."

* * *

In what may be one of the most brazen ripoffs in these parts in recent memory, a company called International Shoppers Spree Inc. called New York telephone numbers with a recorded announcement between October and February. People who picked up the phone heard a high pressure sales pitch urging them to immediately call 540-GOLD so that they could obtain a "gold card". Anyone stupid enough to do this soon found out that their gold card was not the same as an American Express gold card. In addition, the phone call they were urged to make wound up costing $50.20! You see, there's no limit on the amount that these sleasebags can charge for phone calls to their "premium" numbers.

In this case, the Baltimore-based company was ordered to pay a $2,000 fine. They also have to stop what they're doing. Refunds for the suckers are being made available through the New York State Attorney General.

* * *

In Seattle, a TV station showed a half-hour paid ad for a Dial-a-Santa service. The catch: it urged children to call in to a pay line, by holding the telephone up to the TV set while the show played Touch-Tones.

Long Distance Censorship

Yet another threat to BBS operators -- at least one long distance company has taken it upon themselves to decide whether or not the contents of electronic bulletin boards are acceptable. If they decide that they are not, the long distance company will block access to that number! This chilling bit of news comes from Teleconnect, a long distance company based in Cedar Rapids, Iowa. Apparently Teleconnect has blocked access to BBS's that they suspect of having access codes posted on

them.

While the other major long distance companies don't block individual numbers, they all claim that it would be within their rights to do this. They point to the Electronic Communications Secrecy Act of 1986 which states that "phone companies can monitor, intercept, and disclose lines for reasons of non-payment or illegal behavior."

It doesn't take much of a brain to figure out that this legislation is aimed at "direct fraud" like blue boxing or using codes. If a long distance company detects this kind of activity on its lines, they have the right to monitor the line, intercept the conversation, and disclose the phone numbers to the proper authorities (FBI, police, America's Most Wanted, etc.). That is the extent of it. To believe that they can actually prevent the outside world from communicating with someone they "suspect" of being evil is completely wrong. To practice this is not only offensive to democracy, but illegal.

Naturally, we have now put Teleconnect up there with MCI on our official boycott list. We hope that those of you who somehow signed up with Teleconnect manage to "block" their number from your phone because of THEIR illegal actions. And, by all means, add fuel to the fire by reporting all "suspect" numbers immediately to Teleconnect (800-728-7000, ask for Dana). If you find that you're no longer able to reach either the CIA or the NSA on Teleconnect, you can thank us. We had to report them -- the amount of codes those people pass around is staggering.

Foulups & Blunders

The following blurb appeared in recent Florida phone bills:

"You can suspend, restore or disconnect your Florida home telephone service at your convenience with Southern Bell's RightTouch service. You can use RightTouch service 24 hours a day, seven days a week by dialing 1-800-826-6290 from a touch-tone telephone [anywhere in the country]. There is no additional charge for using the service, although the normal charge for restoring your phone service still applies.

"To access RightTouch service, you will need the personal access code (PAC) shown below. This code has been assigned to your telephone number and should be protected as you would a credit card. Once you dial the RightTouch service number, easy-to-follow verbal instructions will guide you through the ordering processing to suspend, restore or disconnect your phone service."

Need we say any more?

* * *

There was a problem with the billing computer at North Caroli-

na State University. It seems that the program used to generate the bills would correctly generate a student's bill, but then address it to the wrong student. The problem was discovered after 6000 bills were mailed to the wrong students.

* * *

An engineer's mistake paralyzed downtown traffic for six minutes in Orlando, Florida last October when signals remained red during lunch hour and forced the city to call out police on horseback to unclog intersections.

Traffic engineers replacing a piece of Orlando's sophisticated traffic light synchronizing system Tuesday forgot to plug in a cable, freezing the signals at 34 intersections, mostly along Orlando's busy north-south thoroughfares just after 12:30 p.m.

"It wasn't a glitch in the system. It was during an installation. Someone forgot to plug in a couple of machines," said mayoral aide Joe Mittiga.

Somehow, that comes across as a glitch to us. A simple human error can cause a snowballing effect when computers are involved. The "glitch" here is the degree to which a computer system can foul up society when one little thing goes wrong.

Abuse. . . .

A British law intended to prevent computer misuse is itself being misused by employers. One of the provisions of the UK Data Protection Act gives individuals the right to obtain copies of information held about them in many computers. But it's being reported that employers are forcing prospective employees to use that right to find out and reveal information about themselves. An example cited is that of local authorities checking up on taxi drivers before granting trading licenses.

Not many of these potential employees are likely to object, since they obviously want the job they're pursuing. And all kinds of information about a person, much of which is not supposed to be anyone else's business, appears in these computers.

Mischief Makers

Michael Banbrook gave his college network managers a scare when he planted a message saying that a virus was active on a college system. Banbrook's message appeared whenever a user mistyped a password. The standard message would be "You are not an authorised user". It was replaced by the brief but sinister "A virus is up and running".

When the message was discovered by the college network manager, Banbrook was immediately forbidden access to any computers at the St. Francis Xavier College at Clapham in South London.

The 17-year-old says that he has uncovered a basic weakness in the college's 64 node RM Nimbus network that runs MS-DOS.

"All anyone has to do is change a five-line DOS batch file," he said.

Banbrook was suspended from computer science classes and forbidden to use the college computers for a week before it was discovered that no virus existed.

* * *

Also in England, a 17-year-old junior cashier cheated the National Westminster Bank out of one million pounds in a computer fraud case. But when the case got to court, Judge Helen Palin criticized the bank for lax security and refused to make a compensation order for the 15,000 pounds which the bank has not been able to recover.

After being given access to the bank's computer system, the cashier began by paying 10 pounds into his own account. He then paid himself 12,000 in imaginary checks. Later, he transferred a credit for 984,252 pounds into the account of a friend and celebrated by buying 50 bottles of champagne.

The judge said, "One of the worrying features of this case is that a young man who hasn't long left school is able to work the system in the NatWest bank on a number of occasions without being found out. Indeed, the general chat within the bank seems to be how easy it is to defraud that bank."

At last, instead of just punishing the ingenious people who figure out ways around the system, we're holding accountable the clods who let it happen.

* * *

Lab Notes: "An unauthorized user copied and modified password files to insert an extra privileged user account and attempted to alter system programs. This incident was noticed at Lawrence Livermore by programmers who took protective actions, and we have notified other sites that were affected."

2600 Marketplace

LEARN ABOUT SATELLITES, DESCRAMBLING, CABLE TV! Read The Blank Box Newsletter, 100 Bride St., #27, Hot Springs, AR 71901 or call 501-321-1845.

DESPERATELY NEED COPY of "Inside Commodore DOS" by Gerald Neufeld and Richard Immers. Will Buy, trade, etc. for same. Fred A. Gingher, PO Box 10132, Wilmington, DE 19850.

FOR SALE: DEC VAX/VMS manuals for VMS 4.2. This includes ALL manuals (systems manuals and users guides) and those orange binders. Contact me for more info. Kurt P., PO Box 11282, Blacksburg, VA 24062-1282.

WANTED: Text files / Countlegger/ Phrack news clippings on hackers, phreaks, etc. from newspapers and magazines. Willing to pay or trade. Send a list to KH, N. 11107 Roundup, Mead, WA 99021.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid via UPS or First Class Mail. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

APPLECAT: I need the touch-tone decoder chip and software for an Apple Cat 202. If you have one to sell, please post to S. Foxx, 430 Dundee Drive, Blue Bell, PA 19422-2440.

WANTED: Any hacking, phreaking software for an IBM computer, also red and blue box plan, vending machines lock pickgun/tools. I will pay good cash for any of the above. Send all info to Mr. Griffith, 25 Amaranth Crt, Toronto, ONT Canada M6A 2P1.

WANTED: Any hacking programs for the Atari ST. Will trade. Also in need of good blue box plans. Would love to hear from other persons interested in P/H from Lexington, KY. Aristotle, 606-258-2219.

COMPUTERIZED LEARNING USER'S GROUP, ELECTRONICS is for those interested in learning electronics and related technologies as well as those interested in developing, evaluating, sharing, and selling hardware and software to do so. Write CLUGE, 207 East School Street, Kent, Ohio 44240-3837 or call 216-678-4611.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

WANTED: Red box and/or blue box, tone chips for making boxes, Macintosh software for trade via mail or modem and vending machine lockpick gun/tools. Douglas, PO Box 8022, Richmond, IN 47374.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info or to request a meeting in your city.

Deadline for Summer Marketplace: 6/1/89.

(continued from page 35)

these stations are not very secure, in some cases made from nothing more than plastic. In some units, the touch tone access is available, yet the telephones are not configured to accept 950 calls as toll-free, again inconveniencing the customer.

The Telco copies are not much better. Operator assistance is limited to that which can be obtained from home lines. Again, calls cannot be completed through long-distance carriers since the station is not configured to accept toll-free 950 calls, although these telephones are usually configured to allow AT&T calling card calls (0+ calls) to be placed through it.

The Cheese Box

There are files circulating about the modem/phreak world regarding a device known as a cheese box. According to the files, when one forwards his number to an Intercept Operator within his prefix, all subsequent outgoing calls made will be prompted for coin insertion, supposedly turning the subscriber's telephone into a payphone. It should be quite obvious that this is impossible, since not only does the Intercept Operator have nothing to do with payphones, coin accounting, and ACTS, but it also seems quite impossible that one's line could become interfaced with ACTS simply by forwarding it to an operator. Obviously, these files are bogus.

Phone Abuse

In this last section, I will discuss how you can use the knowledge obtained from above to use to your advantage when dealing with these telephones. I am not going to get into such topics as phone theft and vandalism -- I'll leave that up to your imagination.

The main advantage of the payphone, to the phreak, is that it provides anonymity. This makes the payphone a perfect location for blue boxing, engineering operators, and other Telco employees, modeming (for the more daring), and general experimentation.

Yet, perhaps the most famous aspect of phreaking regarding the payphone is the use of the red box. As mentioned above, the red box is used to simulate the tones that signal ACTS that money has been deposited in the phone and ACTS may place the call and begin billing (if service is timed). The red box is used by dialing the desired number first and then, when ACTS asks for the change, using the red box to send the coin signals. In an attempt to stop red boxing, the payphone checks to see if the first coin is real, by conducting a ground test. To circumvent this, at least one coin must be deposited -- a nickel is sufficient. However, the number must be dialed first since ACTS must return your coins before reminding you that you have insufficient credit to place the call. Afterwards, any

IN DETAIL

subsequent deposits required can be red boxed successfully, and the duration of the call can be as long as you like.

Red box schematics have proven to be hard to come by and are notoriously a pain to build, not only in the somewhat more complex circuit design than the simple tone generators used in blue, beige and similar boxes, but also in the fact that they are hard to tune precisely, since not only is a frequency counter needed, but also an oscilloscope, both of which are hard to come by and are very expensive.

However, there are alternatives. One method is to locate a payphone that produces the coin deposit tones quite loudly when coins are inserted. You can then record the tones with a Walkman (I do not recommend a micro-cassette recorder for this, because they are not stable enough for the precision required by ACTS) and simply play them back into the mouthpiece when you want to place a call just as you would if you had an actual red box. When you record the tones, record mostly quarters, since, obviously, they are worth the most calling time.

But if you don't have your trusty Walkman with you, there is still another way. Simply find a set of two payphones (or more) with at least one that generates loud coin deposit tones. This phone will be Phone A. Now dial the desired number in Phone B and when ACTS asks you for the amount required, deposit a nickel in Phone B. Now put the two handsets of the phones together (the wires are long enough to reach across the booths) with the earpiece of Phone A held tight against the mouthpiece of Phone B. It doesn't matter where the other two ends are. The purpose of this is to get the sound of the deposit tones from Phone A's earpiece into the mouthpiece of Phone B. Then simply keep depositing coins in Phone A until ACTS thanks you for using AT&T. If you were smart, you only used quarters in Phone A, so you could get some credit towards overtime. Since a number was never dialed with Phone A, when you hang up, all the change will be returned to you.

Red boxes are very useful but

2600 Meetings

First Friday of the month in the lobby of the Citicorp Center, 53rd Street, between 3rd and Lexington, NYC, from 5pm to 8pm. Casual attire please. More info: 516-751-2600.

not convenient for local calls, though they will, of course, work. Another method for placing local calls free of charge is very similar to what David did in War Games to the payphone. The problem with that method is that Telco has now sealed all mouthpieces on the payphones. However, by puncturing the mouthpiece with a nail, the metal inside it will be exposed. There are two variations on this "nail" or "paper clip trick", depending on the telephone in use.

On the older D-types, by either placing a nail or a paper clip in the hole made in the mouthpiece and then touching the other end to any metal part of the phone, a short circuit will occur which will render the keypad inoperable. If this is the case, then dial all digits of the number except for the last as you would normally and then short circuit the phone. While doing that, hold down the last digit of the number, disconnect the "jumper" you have made and then release the key. If this doesn't work, try rapidly connecting and disconnecting the jumper while holding down the last digit. The call should then be placed. What happens is the short circuit causes the coin signaler to malfunction and send a coin signal, while also shorting out the station, so that it passes the ground test.

On the newer payphones, the short circuit will not deactivate the keypad. In this case, simply short circuit the phone throughout the entire dialing procedure and once completed, immediately and rapidly connect and disconnect your "jumper", which, if done properly will allow the call to be placed.

A more direct approach to payphone abuse is actually making money from it. To accomplish this, you need access to the line feeding the telephone. This is often easiest in cases when the telephone is in a location that is below ground and the main distribution cable is in the ground above the telephone's location, such as the lower levels of buildings and subways. If you are able to get to the wires, then cut them, or least one, so that the dialtone has been lost. Wire colors are irrelevant here since I have seen many different colors used, ranging from blue to striped multicolor. By cutting wires, you should have the effect of cutting all power to the phone. When someone walks up to the telephone, he doesn't usually listen for a dialtone and simply deposits his quarter. The quarter then falls into the hopper, and since there is no power to cause a line reversal, the relay will not release the coin. The coins can then be retrieved by reconnecting the wires and flicking the switchhook to initiate a line reversal, which will result in a coin return.

A word of warning: Telco monitors their payphones and knows when to expect the coin box to be

full. Computer-based operations systems aid collection by preparing lists of coin boxes that are candidates for collection, taking into account location and projected activity. The coins collected are counted and entered into the operations system. Discrepancies between actual and expected revenue are reported to Telco security, which investigates them and reports potential security problems. Routine station inspections are also performed during collection, and out-of-service or hazardous conditions are reported immediately for repair.

The privately owned electronic payphones are just as susceptible to attack, if not more so. Most notably, just by hitting the digital ones hard enough in the area of the coin slot sometimes causes the payphone to enter a "Maintenance Mode", where the LCD display shows something to the effect of "Not in Service - Maintenance Mode" and then prompts you for a password, which, when entered, places you in a diagnostic/maintenance program.

Another notable weakness lies in the touch tones the digital telephones produce when it places a call through the PBX. If you can record them and identify them, you will have a number and working access code for the PBX used by the telephone. Identification of the tones is rather difficult, though, since they are sent at durations of 50ms.

Perhaps even more interesting with these phones is that the operator will not identify the phone number you are calling from. She does, however, appear to have ANI capabilities, since one operator confided that she knew the number, yet was not allowed to release it. There is a reason for this. These telephones can be serviced from remote, being equipped with an internal 300 baud modem. The phones enter the "Maintenance Mode" when they are connected to, and are therefore "Out of Service", as the display shows. Others will enter a "Maintenance Mode" only at a specific time of day, when activity is lowest, and only then can they be reached. From remote, diagnostic functions can be performed, as well as the ability to poll the unit to determine the amount of money in the coin box, plus an accounting of local and long-distance calls, though these functions will, of course, differ from phone to phone.

The "Telco copies" also contain a 300 baud modem. Since ANI is locked out from the keypad, the number can only obtained through the operator; she is not aware that you are calling from a payphone, since the station has been installed on a standard customer line. Since 0+ calls are available through this unit, Directory

(continued from page 29)

are you sure this is what you want to do? In other words, do you owe these people anything? And are you expecting something in return? Odds are you won't get it.

Regardless of how you choose to handle this, your life is not over. You're having a very unpleasant experience, granted. But you will recover from it and you will benefit from it if you try. Be honest and open and reach out to others as you have in this letter. Don't concentrate on how miserable things are and on what opportunities have been lost. If you acknowledge your mistakes and refuse to let them defeat you, anything is still possible.

Please keep us updated as to your situation.

TO SEND A LETTER TO 2600, DO THE FOLLOWING:

1) Write it.

2) Mail it to us through the U.S. mail. Our address is:

2600
PO Box 99
Middle Island, NY
11953-0099

SCRAMBLE FACTS

A three minute program devoted to news and views, technical tips, and new product information. The contents are specific to the TVRO (television receive only) industry (satellite TV for the home owner).

(718) 343-0130

(costs only a phone call)

PAYPHONES

Assistance can be obtained for free by dialing 0-NPA-555-1212. Since the telephone is configured not to charge for calls placed with 0's before them (to allow for calling card calls) the call is free.

Conclusion

I have tried to make this article as informative and accurate as possible, obtaining information from various manuals as well as personal experience. Since payphones are public, the best way to learn about them is simply to experiment with them on your own. Good luck.

NOW HEAR THIS

At 2600, we don't exactly go out of our way to nag you about when your subscription is going to end. You won't find yourself getting those glossy reminders with free pens and digital quartz clocks and all that crap. We believe our subscribers are intelligent enough to look at their address label and see if their subscription is about to expire. If it is or if you want to extend it, just fill out the form below (your label should be on the other side) and send it to our address (also on the other side). You don't get self addressed stamped envelopes from us. But the time and money we save will go towards making 2600 as good and informative as it can be.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25

TOTAL AMOUNT ENCLOSED: [ ]

In These Pages...

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Permit Issued at
East Setauket, N.Y.
11733

ISSN 0749-3851