A Guide To Breaching HP 3000 Security

Phil Curry
Carter, Schaefer & Company
Houston, Texas

Introduction

People have been intrigued by secret codes and security for years. Take for example the decoder pins given away as premiums during the 1930's. A kid with his Captain Midnight or Little Orphan Annie decoder pin could send a "secure" secret message to his or her pal and keep would be "spies" from deciphering the message.

In the 1980's people are no different. With a relatively cheap computer or terminal one can try their hand at breaking security on a computer system. Most of the time it's not that the computer system has anything of any real value, it's just the fun of breaking the security and finding the codes to get into the computer.

What I'm going to reveal about you Hewlett Packard 3000 computer systems will make most system managers weak and wonder why in the world am I telling everyone this. The answer is simple. To prevent you from having a breach of security. Chances are you have already had a breach and never knew it. I'm not necessarily talking about someone logging on and moving money into their checking account or changing their hourly pay rate. I'm talking about someone having access to your system and potentially having this capability without your even knowing it. Someone may know they can have access to your computer or system account anytime they wish and are waiting for the right time to use it, like one week after they are layed off work or fired.

What this paper will do is give you an idea of how a Hacker thinks and can gain access to your system. It speaks from the view of the Hacker and tells how you as the system manager can prevent the breach of security. In some cases, one can't. Also note that I'm not giving away all my secrets. Like a magician I must keep the mystique of knowing how to get into a system to myself. Their are ways that if told could do more harm than good.

There is a misconception of what a Hacker really is. A Hacker is not one of these kids seen in movies like War Games that attempts to call computers and break into them. The name they give themselves is "Phreaks". A Hacker is a one who really gets down to bits and bytes with the computer.

Real Hackers.....

1. patch the object code. It's much faster than the edit, compile, and prep process.

2. use the ASSEMBLE statement in SPL.

3. can perform Binary, Octal, Hex, and Decimal conversion in their head.

4. know at least 4 languages (at least 5 if you count Basic).

I'll now remove my system manager hat and put on my Hackers hat and reveal how you can potentially break security on an HP 3000. Again, note that this is done to tell you how to prevent a breach and NOT to let people know how to get into your system.

Chapter I - Gaining Access To An HP 3000

The first thing one needs to do to breach security on an HP 3000 is to get access to one. If you have access to a personal computer and an autodial modem, you can do this.

In the movie "War Games", a high school student uses his home computer (an archaic Imsai 8080) to dial successive numbers in a telephone exchange looking for modems. You can do this too! There are many "War Games Dialers" available on computer bulletin board systems. If you can't find one, their easy enough to write. Anyone can go to Toy's Are Us and buy a Commodore 64 computer and a modem and do exactly what was done in the movie to find modem numbers to computers. Looking at the figures in the March 30, 1987 issue of Infoworld magazine, IBM has sold over 7 million personal computers. In early 1988, IBM announced they have sold over 1 million PS/2s, which raises the number to over 8 million. This figure doesn't even count compatibles, such as Compaq. Considering the cost of these systems, imagine how many less expensive Apple and Commodore computers are in the marketplace. Any one of these computers with a modem can access an HP 3000.

Some system managers are crafty and will buy modems that will not run at lower speeds to keep cheap 300 and even 1200 baud modems from connecting to their system. Even harder to overcome is the use of dial-back modems. Whenever someone wants access to the computer they must enter their name or access code. Then the line is disconnected and the computer calls the phone number it has stored for the password and connects to the terminal or computer. This keeps one from hacking into the system since even though we know a password, the computer will hang us up and dial the number it has associated with the logon.

Chapter II - You Have A Colon Prompt, Now What?

Ok, you now have access to an HP 3000. Now you need to log on to it. You need to know a user and account that is on the computer system. Hear are some user.account combinations to try:

MANAGER.SYS	Password: HPONLY
OPERATOR.SYS	
MGR.TELESUP	Password: HPONLY
FIELD.SUPPORT	Password: HPONLY
MGR.MAINLIB	
MGR.CSL3000	
MANAGER.TECH	
MGR.INTX2	
MGR.SCRUG	
MGR.BWRUG	
MGR.DETROIT	
MGR.GAMES	

If you already have a valid account on the system you're way ahead of the game.

To keep you from finding out passwords, good system managers will never use default passwords, HP's or third party vendor's. Passwords may be hard to guess since the best passwords are meaningless, like license plates. Combinations of letters and numbers not the name of the user's child or dog. Also three passwords could be needed; account, user and group.

Chapter III - Your On The Computer, Now What?

If you didn't log on as MANAGER.SYS or FIELD.SUPPORT you will have limited access to the computer. You want as much access as you can get. You can do the following things to find other person's passwords.

I. The Fake Restore

The MPE Store format is documented in the Systems Managers Reference Manual. The STORE command will disallow one from restoring files from one account into another. However, what you can do is write a program to read the STORE tape and load the files into your account. Program files are no good. The good ones will need to be run in an account with PM capability anyway. Good files are CATALOG.PUB.SYS and any file that looks like a stream file (files in groups named JOB). Don't let lockwords scare you, they are just part of the data on the tape. If you have a SYSDUMP tape, that's even better since the system directory is on the front of the tape. Get a source code listing of STAN from the Contributed Library, it can help immensely.

After you've written your program, tell the operator that you accidently purged a file and need to restore it from the last backup tape. Tell him you'll do the RESTORE command when he mounts the tape. Then run your program and the unsuspecting operator will mount the tape and reply to it.

II. Intercept Terminal I/O

Look for the program called PEEKABOO. This contributed program allows one to monitor all terminal activity to a device. For example, you can run PEEKABOO on the console, device 20, or on the system manager's port.

III. The Fake Prompt Trick

Write a program to emulate the MPE command interpreter. The steps are as follows:

1. Open file on another terminal
2. Read device.
3. If input is not a HELLO command send appropriate error message and go to step 2.
4. Scan for missing passwords (user didn't enter password during logon)
5. Prompt for password(s)

6. Give fake MPE error message (such as account out of time, cannot open UDC catalog, etc.)
7. Close the terminal.
8. Write the passwords to a file to read later.

You can get as elaborate as you wish. You could even fake a logon and parse the users commands and any of them that are programatic (LISTF, REPORT, SHOWJOB, etc.).

IV. The Trojan Horse

Write a GREAT program that is a game or utility that alot of people will run. When the unsuspecting system manager puts it in an account where everyone can run it, you can get their passwords. The steps are as follows:

1. Do a programmatic LISTUSER to a RELEASED file in your account. Be sure the file equation for the LISTUSER accesses the file with append access. If the command fails, then the password is of little value since it doesn't even give you account manager capability, proceed to step 3.
2. Do a programmatic LISTACCT to the RELEASED file in your account. The command won't fail since the program got this far. Also, if the user has SM capability, you just got ALL account passwords.
3. Begin game or utility program.

V. The Terminal Emulator Trojan Horse

A good terminal emulator is hard to write, but you can write a simple one. Some are available with source code, like KERMIT, from local bulletin boards or personal computer user groups. Once you have the program, some simple modifications will help you get other user's passwords. What you do is give a copy of the program to someone who has a password to the system that you desire. Remember, the program you gave them sees EVERYTHING the user types. So, what you do is write code to look for the user's logon and the MPE welcome. You will need to write another program on the HP 3000 and release it. The HP 3000 program will perform a file transfer by doing the following:

1. Reads the terminal until some end of file indication.
2. Appends the HELLO command and accompanying passwords to a RELEASED file in your account.

On the PC end, your emulator will need to do the following:

1. Look for HELLO command
2. Look for MPE welcome with revision of the operating system and terminal read.
3. Issue command to MPE (remember, you have control) to run your program described above.
4. Transfer logon information to the HP 3000.
5. Begin normal terminal emulation.

VI. Use Unknown Bugs Or Features Of Programs

The program SLS is a widely used program from the Contributed Library. It allows one to stream jobs while interacting with the user for information before doing the STREAM. The program writes the stream file to a file named JXXXA then calls the COMMAND intrinsic with the command STREAM JXXXA then purges the file. The original source does not disallow file equations to the file JXXXA so by doing the following you can see the passwords in the stream file:

1. :FILE JXXXA=$STDLIST
2. Now do the normal steps to do the SLS job
   Example: :SLS BACKUP

The entire JOB stream, including passwords will be displayed on your terminal.

If the system manager has locked you out of using the compilers or system utilities such as FCOPY, PREP or RELEASE, find access to a utility that allows programmatic calling of these commands or allows running programs inside them. Good examples are EDITOR, QUAD, and SPOOK. Try putting a colon in front of the command if just typing the command does not work. QUAD gives you access to the compilers as well as MPE commands so it is a good choice.

There are some other undocumented features on the HP 3000 that are interesting.

1. In QUERY, after doing a FIND type the command NUMBERS. This will display the relative record numbers of the records you just found.

2. In EDITOR when saving a file and asked if you wish to "PURGE OLD?" you can enter "OK" in place of "Y".

3. Most HP utilities will let users with PM capability to type DEBUG at the prompt and will drop them into PRIV MODE DEBUG.

4. There is a program in PUB.SYS called IOCDPNO that is disguised as a card punch driver left there for SE's to be able to call ATTACHIO directly. If you enter HELP at the prompt, you can cause a system failure.

5. There used to be a back door in MPE. You could type =DEBUGG (yes, two g's) at the console at drop right into PRIV MODE DEBUG.

If programmers at Hewlett/Packard are allowed to leave undocumented commands in the software, there just may be some back door waiting to be found.

VII. Look For Files In PUB.SYS And Other Accounts You Can Run

Most system managers have no idea what is in PUB.SYS. Unless otherwise altered, most programs in this group can be run by everyone. Sometimes, the lazy system manager will put utilities in this group so several people can run 1 copy of the program and hope user ignorance will keep others from running the program. Some useful programs to look for include:

1. PEEKABOO
2. ALLOWME
3. STAN
4. GOD
5. JSPOOK

Also, look for any released program files in PUB.SYS. You can write a program with PRIV MODE capability and copy it on top of the RELEASEd file.

1. Write PRIV MODE program and compile it.
2. PREP without PM capability (you need PM to PREP with PM)
3. Patch the object code to give program PM capability. You can do this with DECOMP from the Contributed Library using the REPREP command.
4. FCOPY released program to your account.
5. Copy your program on top of RELEASED program file.
6. Run program.
7. FCOPY original file back (destroy the evidence).

Epilog - What Have We Learned?

Now I'll take off my Hackers hat and put my system managers hat back on and re-cap what we learned.

1. Be careful who is dialing into your computer system. If really necessary, use dial-back modems to verify the user.

2. Put passwords on ALL accounts no matter how little access they have. Once a person is on, they could access things you never thought of. And NEVER leave the passwords on the accounts SYS and SUPPORT at their default.

3. Do not mount SYSDUMP or STORE tapes for users to read. If a user lost a file, RESTORE it for him.

4. Don't keep PEEKABOO lying around.

5. When logging on, suspect that you have a fake colon prompt when logging onto the machine. Type :EOF: to close the device, then press RETURN to get another prompt.

6. Never take programs written by users and place them in accounts where all users can run them unless you have source code. Then, recompile the program and put THAT object code where everyone can run it. Sometimes this isn't possible, like Contributed Library programs. BEWARE of persons bearing gifts.

7. Limit access to the MPE command interpreter to users. As you can see, this is where all the trouble starts. Get a menu system and allow users to only run what is needed. You can pass it off as a "User friendly interface" and get away with it.

8. Look at all files in accounts everyone has access to. Make sure none of them are RELEASED. Make the access to the file minimal. For example, utilities like SLPATCH should have its access X:CR to allow access only by the creator, not everyone.

9. Don't place anything in PUB.SYS that didn't come from HP. Utilities should go in a different group and maybe a different account if no PRIV MODE is needed.

10. Security is a never ending battle.

Appendix
Listing Of A "War Games Dialer"

```
10 '*******  AUTOMATIC SEQUENCE DIALER (a la "Wargames") **********************
20 'Written for the IBM PC and HAYES SMARTMODEM by Steve Klein 9/25/83
30 'Modified (Steve wouldn't recognize it anymore) with enhancements (starting
40 'number, printer on/off option, abort/hang up) by John Siers 12/28/83
45 '*****************************************************************************
50 'This program will dial numbers in sequence looking for computer carrier
60 'signals. When carrier is found, phone # is listed to printer and/or screen.
75 '*****************************************************************************
100 CLEAR ,,2000:XY=2
110 KEY OFF:COLOR 0,7:CLS:LOCATE 10,25:PRINT "Wargames Dialer Program"
120 LOCATE 12,26:PRINT "Written by Steve Klein":LOCATE 14,26:PRINT "Modified by
John Siers"
125 FOR I=1 TO 5000:NEXT
130 A$="":AB$="":CLS:PRINT " PLEASE ENTER PREFIX DIGITS (IF ANY), THE AREA CODE
(IF ANY), AND THE":PRINT "FIRST THREE NUMBERS [hyphens may be used to separate
e.g.9-1-nnn-nnn]: ":INPUT "~~~>",A$
140 INPUT "START DIALING AT # (LAST 4 DIGITS)";SN:IF SN>9999 OR SN<0 THEN 140
ELSE N1=INT(SN/1000):N2=INT((SN-(N1*1000))/100):
N3=INT((SN-(N1*1000+N2*100))/10):N4=SN-(N1*1000+N2*100+N3*10)
160 PRINT "LIST COMPUTER CONNECTIONS TO <S>CREEN ONLY OR <P>RINTER AND SCREEN?"
170 PRINTON$=INKEY$:IF PRINTON$<>"S" AND PRINTON$<>"s" AND PRINTON$<>"P" AND
PRINTON$<>"p" THEN 170
200 '*** Begin dialing sequence ***
205 CLS
210 FOR E=N1 TO 9:FOR B=N2 TO 9:FOR C=N3 TO 9:FOR D=N4 TO 9:N1=0:N2=0:N3=0:N4=0
220 OPEN "COM1:300,n,8,1,CS,DS" AS #1:R=32:PRINT #1,"ATDT"A$;E;B;C;D
225 DIAL=E*1000+B*100+C*10+D:DL$=STR$(DIAL):IF LEN(DL$)=2 THEN DN$="000"+
RIGHT$(DL$,1) ELSE IF LEN(DL$)=3 THEN DN$="-00"+RIGHT$(DL$,2) ELSE
IF LEN(DL$)=4 THEN DN$="-0"+RIGHT$(DL$,3) ELSE DN$="-"+RIGHT$(DL$,4)
230 GOSUB 500:LOCATE 25,1:PRINT "DIALING ";A$;DN$;:LOCATE 25,35:
PRINT "TIME LEFT";R;"SECONDS: [A]=ABORT [H]=HANG UP ";
240 '*** Check for input to comm buffer (carrier) ***
250 A=LOC(1):IF A>(20+LEN(A$)) THEN 280
260 IF R>0 THEN 230
270 CLOSE:FOR I=1 TO 3000:NEXT:NEXT D,C,B,E
275 LOCATE 25,1:PRINT STRING$(79,32);:LOCATE 25,1:
PRINT "END OF DIALING SEQUENCE:";:INPUT " PRESS ENTER TO CONTINUE ---->";XX$:
GOTO 130
278 '*** Found One!!! ***
280 SOUND 150,5:XY=XY+1:LOCATE XY,1:PRINT A$;DN$:IF PRINTON$="P" OR
PRINTON$="p" THEN LPRINT A$;DN$
290 GOTO 270
500 '*** Countdown time and check for abort/hang up ***
510 LET R=R-1:FOR I=1 TO 1050:NEXT:AB$=INKEY$:IF AB$="A" OR AB$="a" THEN 520
ELSE IF AB$="H" OR AB$="h" THEN 530 ELSE RETURN
520 PRINT #1,"ATH":CLOSE:LOCATE 25,1:PRINT STRING$(79,32);:LOCATE 25,1:
INPUT "DIALING ABORTED: PRESS ENTER TO CONTINUE ---->";XX$:GOTO 130
530 PRINT #1,"ATH":R=0:RETURN
1000 '*****************************************************************************
1010 ' Another helpful program from Steve Klein
1020 ' With enhancements by John Siers (who found the original on the
1030 ' Lehigh Valley BBS, Allentown PA -- 12/83)
```