Is Your Homestead Secure?

(Keeping your e3000 safe from hackers until 2006 or beyond)

Mark Bixby
TCSD/vCSY
March 27, 2003

Presentation overview

- Getting started with security on MPE
- Auditing
- Authentication
- Authorization
- Networking (general and product-specific)
- :STORE/:RESTORE
- Denial of service
- People & processes
- The future
- Real-life security stories from the audience
- General Q&A

Getting started with security on MPE

Security-related documentation

- Accessing Files Programmer's Guide
- New Features of MPE/iX: Using the Hierarchical File System (see also :XEQ POSIXCBT.LSN.SYS)
- Performing System Management Tasks
- Manager's Guide to MPE/iX Security
- User's Guide to MPE/iX Security
- HP Security Monitor/iX Manager's Guide
- HP Security Monitor/iX User's Guide

System logging

- Enabled via :SYSGEN
- Logging event data written to LOG#####.PUB.SYS
- :SHOWLOG – displays current log file
- :SWITCHLOG – switches to a new log file
- Use LOGTOOL.PUB.SYS or third-party utilities to display key logging events periodically
- Enable as many logging events as you can!

System logging events

- 100 - System Logging
- 101 - System Up
- 102 - Job Initiation
- 103 - Job Termination
- 104 - Process Termination
- 105 - NM File Close
- 106 - System Shutdown
- 107 - Power Failure
- 111 - I/O Error
- 112 - Physical Mount/Dismount
- 113 - Logical Mount/Dismount
- 114 - Tape Label

System logging events (cont.)

- 115 - Console Log
- 116 - Program File Event
- 120 - Native Mode Spooling
- 121 - File Quarantine Event
- 127 - Chdir
- 128 - Process Adoption
- 129 - File Owner Change
- 130 - Architected InterFace
- 131 - Additional Processor Launch
- 134 - Password Change
- 135 - System Logging Configuration
- 136 - Restore

System logging events (cont.)

- 137 - Printer Access Failure
- 138 - ACD Change
- 139 - Stream Initiation
- 140 - User Logging
- 141 - Process Creation
- 142 - Security Configuration Change
- 143 - Chgroup
- 144 - File Open
- 145 - CI Command Logging
- 146 - Maintenance Request
- 148 - UPS Monitor Event Logging

System logging events (cont.)

- 150 - Diagnostic Information
- 151 - High Priority Machine Check
- 152 - Low Priority Machine Check
- 155 - Directory Open/Close Logging
- 160 - CM File Close

Auditing

There's more than just the console and system logging

- Many subsystems use separate logging facilities:
  - INETD – JINETD $STDLIST spoolfile
  - Apache - /APACHE/PUB/logs
  - DNS BIND/iX – syslog (and possibly the console)
  - Samba - /usr/local/samba/var
  - Sendmail – syslog (and possibly the console)
- Home-grown applications?
- Third-party applications?
- ALL logs need to be checked periodically for anomalies

Where did that :HELLO come from?

- System logging and console messages don't include the IP address for terminal logons/logoffs
- A system logon UDC could be used to capture the HPREMIPADDR CI variable for successful logons
- But there is currently no way on MPE to capture the IP address of a failed VT-MGR logon attempt
- Enable INETD connection logging option (-l) to track all telnet connections
- Use external firewall SYN logging?

Which files have been :RELEASEd?

- :RELEASE is a great convenience for relaxing file security, but it opens major security holes
- There are no FOS tools to conveniently scan for :RELEASEd files, but you can do this from the CI:

```
file temp;rec=,,b;disc=2147483647
listfile /,3 >*temp
xeq awk.hpbin.sys "'&
$1 == ""FILE:"" { file=$2 } &
/SECURITY IS OFF/ { print file}'" <*temp
purge *temp;temp
```

- Then :SECURE any items that no longer need to be :RELEASEd

Which files are world-writable?

- World-writable files are equally risky
- To search for all world-writable files using the POSIX shell:

```
find / -perm -o+w -a ! -type l | xargs ls -ld
```

- Then tighten security if appropriate

Who is using special capabilities (I.e. SM, OP, PM)?

- No FOS tools for conveniently auditing special capability usage
- Vesoft's VEAUDIT/3000 product does a good job
- You could scan :LISTACCT, :LISTUSER, :LISTGROUP output for account, user, and group usage
- You could scan VERSION.PUB.SYS output for program file usage

Listing all users with SM, OP, or PM capability

```
file temp;rec=,,b;disc=2147483647
listuser @.@ >*temp
xeq awk.hpbin.sys "'&
/^USER:/ { user=$2 } &
/^CAP:.*(SM|OP|PM)/ { print user}'" <*temp
purge *temp;temp
```

Listing all PROG files with PM capability

```
file temp;rec=,,b;disc=2147483647
listfile @.@.@,6;seleq=[code=prog] >*temp

file temp2;rec=,,b;disc=2147483647
xeq version.pub.sys <*temp >*temp2

xeq awk.hpbin.sys "'&
/^VERSION>/ { getline; getline prog } &
/^CAP:.*PM/ { print prog }'" <*temp2

purge *temp;temp
purge *temp2;temp
```

Listing all NMPRG files with PM capability

```
file temp;rec=,,b;disc=2147483647
listfile @.@.@,6;seleq=[code=nmprg] >*temp

file temp2;rec=,,b;disc=2147483647
xeq version.pub.sys <*temp >*temp2

xeq awk.hpbin.sys "'&
/^VERSION>/ { getline; getline prog } &
/^CAPABILITIES:.*PM/ { print prog }'" <*temp2

purge *temp;temp
purge *temp2;temp
```

Who can write to priv-mode groups?

- Non-prived users who can write to CAP=PM groups essentially have priv-mode capabilities
- Make sure group-level security has restricted write and save access to authorized users
- Make sure program files in PM groups are not :RELEASEd or writable by by unauthorized users
- Process :LISTACCT/:LISTGROUP/:LISTFILE output yourself, or just purchase Vesoft's VEAUDIT/3000

Would you know it if a hacker replaced a system file with a trojan horse?

- Monitor system logging for unauthorized file open/close events
  - but what if a hacker disabled system logging or sanitized the log files?
- Build a database of file checksums and other attributes for comparison purposes to detect file changes
  - Update the database after legitimate file changes
  - Various open source solutions – TripWire, Osiris, etc

Tracking account/user/group object changes

- Would you be able to tell if a hacker assigned SM or PM capability to some obscure user?
- Periodically compare :LISTACCT, :LISTUSER, :LISTGROUP output looking for any differences
- Purchase HP Security Monitor/iX and enable command logging for :NEWACCT, :NEWUSER, :NEWGROUP, :ALTACCT, :ALTUSER, :ALTGROUP

Command file SNAPU – taking a snapshot of user attributes

```
file temp;rec=,,b;disc=2147483647
listuser @.@;format=detail >*temp
xeq awk.hpbin.sys "'&
/^USER/ { user=$3 ; next } &
/^(LOGON CNT|\*)/ { next } &
 { sub(/ *$/,"""",$0); &
   printf ""%-17s %s\n"",user,$0 }'" <*temp
purge *temp;temp
```

SNAPU output

```
OPERATOR.SYS      PASSWORD    : **
OPERATOR.SYS      UID         : 142
OPERATOR.SYS      GID         : 1
OPERATOR.SYS      MAX PRI     : 150
OPERATOR.SYS      LOC ATTR    : $00000000
OPERATOR.SYS      HOME DIR    : /SYS/OPERATOR
OPERATOR.SYS      LOGON CI    : /SYS/PUB/CI
OPERATOR.SYS      CAP         : GL,OP,UV,LG,ND,SF,BA,IA
```

Compare SNAPU output to detect changes

- **:SNAPU >before**
- **:save before**
- …time passes…
- **:SNAPU >after**
- **:save >after**
- **:xeq diff.hpbin.sys 'BEFORE AFTER'**

```
2304c2304
< OPERATOR.SYS      CAP          : GL,OP,UV,LG,ND,SF,BA,IA
---
> OPERATOR.SYS      CAP          : GL,OP,UV,LG,ND,SF,BA,IA,PM
```

System logging event #115 gives incomplete picture of console activity

- Only a subset of CI commands are logged by event #115
- Enable additional logging events to get a better picture of console activity
- If you are really paranoid, purchase HP Security Monitor/iX and enable CI command logging for all commands and all users (might be overkill!)

Perform periodic packet sniffing

- :NETCONTROL TRACEON/TRACEOFF to capture packets, and :NMDUMP to format them
- :NMDUMP is cumbersome and overly verbose, so using external packet sniffing tools might be a better choice
- Connection attempts to unused TCP or UDP ports can indicate hacker scanning activity

Auditing events across distributed systems

- A single transaction may easily span multiple systems, each with their own clock of varying accuracy
- Run NTP or other time synchronization software on each system so that event timestamps on one system may be correlated reliably with event timestamps on another system
- NTP for MPE: http://jazz.external.hp.com/src/hp_freeware/ntp/

Strange network errors may be a sign of hacker scanning tools

- Some common hacker tools such as Nessus (www.nessus.org) are aware of MPE
- These tools scan for used TCP or UDP ports and then probe for known vulnerabilities
- Unusual console messages typically result, either a few or a flood

Nessus example console messages

```
14:18/#J89/174/Could not receive data from sockets during
  Telnet device initialization
14:18/#J89/174/Call to initialize telnet server failed with
  error -7
** NS/3000 NetIPC ERROR IN VT; Job: 0; PIN: 239; Info: 1
- Error: 42;
** NS/3000 NetIPC ERROR IN VT; Job: 0; PIN: 229; Info: 1
- Error: 42;
** NS/3000 NetIPC ERROR IN VT; Job: 0; PIN: 165; Info: 1
- Error: 42;
14:18/160/CAN'T FOPEN $STDLIST IN 'STARTLOGON' ON LDEV #14.
  (js 131)
14:18/160/CAN'T CLEANUP SOCKET ON LDEV #14. (js 89)
14:18/160/CAN'T FOPEN $STDLIST IN 'STARTLOGON' ON LDEV #13.
  (js 131)
14:18/160/CAN'T CLEANUP SOCKET ON LDEV #13. (js 89)
```

Nessus example console messages (cont.)

```
** NS/3000 INTERNAL ERROR IN NFT; Job: 0; PIN: 128; Info: 3
- NFT protocol err: 1
** NS/3000 INTERNAL ERROR IN NFT; Job: 0; PIN: 161; Info: 3
- NFT protocol err: 1
** NS/3000 INTERNAL ERROR IN NFT; Job: 0; PIN: 199; Info: 3
- NFT protocol err: 1
** NS/3000 INTERNAL ERROR IN VT; Job: 0; PIN: 0
- Error: 12; Error Reported by VT
- VT error          : 7; UNEXPECTED/BAD RESPONSE FROM VT
** NS/3000 INTERNAL ERROR IN VT; Job: 0; PIN: 129; Info: 0
- Error: 12; Error Reported by VT
- VT error          : 6; VTS MESSAGE HAS INVALID FORMAT
** NS/3000 NetIPC ERROR IN VT; Job: 0; PIN: 129; Info: 1
- Error: 42;
```

Nessus example console messages (cont.)

```
14:14/#J89/192/FTP INVALID LOGON FOR: "BOGUS" IP=12.34.56.78
14:14/#J89/177/FTP INVALID LOGON FOR: "ROOT" IP=12.34.56.78
14:14/#J89/232/FTP INVALID PASSWORD FOR: "OPERATOR.SYS"
  IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "SPECTRUM.CU1" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "CU1.DBA" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "CU1.MANAGER" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "CU1.MGR" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "CUTEST1.MANAGER"
  IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "CUTEST1.MGR" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "CUTRAIN.MANAGER"
  IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "CUTRAIN.MGR" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "SUPPORT.FIELD" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "SUPPORT.MANAGER"
  IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "SUPPORT.MGR" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "SUPPORT.OPERATOR"
  IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "SYS.MANAGER" IP=12.34.56.78
14:14/#J89/232/FTP INVALID LOGON FOR: "SYS.MGR" IP=12.34.56.78
```

Nessus example console messages (cont.)


```
14:15/#J3/72/Feb 12 14:15:12 localhost sendmail[19595483]: h1CMFCFP19595483:
  IDENT:root@some.hacker [12.34.56.78] did not issue MAIL/EXPN/VRFY/ETRN
  during connection to MTA
14:15/#J3/72/Feb 12 14:15:13 localhost sendmail[27721977]: h1CMFDFP27721977:
  IDENT:root@some.hacker [12.34.56.78] did not issue MAIL/EXPN/VRFY/ETRN
  during connection to MSA
14:18/#J3/72/Feb 12 14:18:10 localhost sendmail[346161297]: h1CMIAFP346161297:
  setsender: |testing: invalid or unparsable, received from
  IDENT:root@some.hacker [12.34.56.78]
14:18/#J3/72/Feb 12 14:18:10 localhost sendmail[116654205]: h1CMIAFP116654205:
  IDENT:root@some.hacker [12.34.56.78] did not issue MAIL/EXPN/VRFY/ETRN
  during connection to MTA
14:18/#J3/72/Feb 12 14:18:10 localhost sendmail[352125066]: h1CMIAFP352125066:
  /tmp/nessus_test... Cannot mail directly to files
14:18/#J3/72/Feb 12 14:18:10 localhost sendmail[25297170]: h1CMIAFP25297170:
  IDENT:root@some.hacker [12.34.56.78] did not issue MAIL/EXPN/VRFY/ETRN
  during connection to MTA
14:18/#J3/72/Feb 12 14:18:10 localhost sendmail[352125066]: h1CMIAFP352125066:
  lost input channel from IDENT:root@some.hacker [12.34.56.78] to MTA after
  rcpt
14:18/#J3/72/Feb 12 14:18:10 localhost sendmail[352125066]: h1CMIAFP352125066:
  from=root@invent3k.external.hp.com, size=0, class=0, nrcpts=0, proto=SMTP,
  daemon=MTA, relay=IDENT:root@some.hacker [12.34.56.78]
14:18/#J3/72/Feb 12 14:18:11 localhost sendmail[76153034]: h1CMIAFP76153034:
  |testing... Cannot mail directly to programs
```

Know your enemies (or know what your enemies know)!

- Download Nessus (www.nessus.org) and other hacker tools yourself
- Perform security scans of your own systems
- Plug any detected holes, but be aware that false positives may be reported
- Scanning during off-peak hours is recommended since these tools can cause certain network services to die on the target machines

Don't get mad, get even!

- Report hacking attempts to the appropriate authorities within your organization
- If the hacking originated via the Internet, use traceroute to display the network topology all the way back to the originating IP address to reveal:
  - the originator's organization
  - the originator's Internet Service Provider
- Visit www.radb.net to determine who owns the netblock containing the IP address
- Complain about the hacking to the organization, the ISP, and the netblock owner

Authentication

Beware of install jobs using blank or constant passwords

- Software product installation jobs (both HP and non-HP) frequently use blank or constant passwords when creating new accounts, groups, and users
- Remember to manually impose custom passwords after software installations
- Periodically check for blank passwords
  - Scanning :LISTACCT, :LISTGROUP, :LISTUSER output
  - Running Vesoft's VEAUDIT/3000 product

Listing users & accounts without passwords

```
comment generate accounts without passwords
file temp;rec=,,b;disc=2147483647
listacct @;pass;format=detail >*temp
file tempa;rec=,,b;disc=2147483647
xeq awk.hpbin.sys "'&
/^ACCOUNT/ { acct=$3 } &
/^PASSWORD/ && NF == 2 { print acct }'" <*temp >*tempa

comment generate users without passwords
listuser @.@;pass;format=detail >*temp
file tempu;rec=,,b;disc=2147483647
xeq awk.hpbin.sys "'&
/^USER/ { user=$3 } &
/^PASSWORD/ && NF == 2 { print user }'" <*temp >*tempu
```

Listing users & accounts without passwords (cont.)

```
comment list users & accounts without passwords
save tempa
save tempu
xeq join.hpbin.sys '-t . -j1 2 -o "1.1 1.2" &
  TEMPU TEMPA'
purge tempa
purge tempu
```

VT/telnet/ftp/dtc authentication sends cleartext passwords over the network

- Any idiot with a packet sniffer can capture these passwords
- Don't use these protocols over an untrusted network (I.e. the Internet)
- Use VPN technologies to transit untrusted networks
- MPE network transport does not directly support any VPN protocols, so you will have to implement them via a firewall/switch/router/etc external to the 3000

Unencrypted passwords in the system directory

- Passwords are stored in the system directory as cleartext by default
- :STORE ;DIRECTORY copies these cleartext passwords to your backup, so control who has access to your backups
- OP users can do :STORE ;DIRECTORY, so control who has access to OP capability
- Purchase HP Security Monitor/iX and enable encrypted passwords
  - one-way encryption is used, so not even SM users can reveal passwords

Generate random passwords in installation jobs

A shell script example:

```
PASSWORD=`echo $$ | awk ' {\
  srand($0);
  for (i=0; i < 8; i++) \
    pass=pass \
         substr("ABCDEFGHIJKLMNOPQRSTUVWXYZ",1+int(26*rand()),1);
  print pass }'`

callci "NEWACCT FOOBAR;PASS=$PASSWORD"
```

Prevent users from choosing weak passwords

- Nothing in MPE FOS to prevent users from choosing blank or weak passwords
- Purchase HP Security Monitor/iX to impose minimum password length requirements
- Purchase Vesoft's Security/3000 to impose minimum length and other password content requirements

Implement password expiration

- Old passwords tend to become shared passwords
- No MPE FOS mechanism for expiring old passwords to prevent them from becoming stale and known by too many people
- Purchase HP SecurityMonitor/iX or Vesoft's Security/3000 to enforce regular MPE user and account password changes
- Don't forget to change database and other passwords too!

Don't use embedded passwords in job streams

- :JOBSECURITY ;PASSEXEMPT= can be used to permit certain classes of users to omit !JOB passwords in batch jobs
- Third-party utilities (Vesoft, others) can insert !JOB passwords prior to :STREAMing

Time-out unattended terminal sessions

- An unattended keyboard with a logged-on terminal session is a security risk
- The HPTIMEOUT CI variable can time-out unattended sessions sitting at a CI prompt
- Various freeware and third-party utilities can time-out idle MPE sessions
- A password-protected PC screen saver can also prevent unauthorized usage

Authorization

The use & abuse of OP capability

- OP capability grants the ability to:
  - :STORE/:RESTORE any file, including the system directory
  - Perform spoolfile and printer management
  - Perform job/session management
  - Use ;HIPRI on jobs
- Few users need ALL of these abilities
- Third-party utilities exist as OP alternatives for spoolfile/printer management and job/session management

Use OP on a temporary, process-local basis

- Use priv-mode AIFs to temporarily give the local process OP capability so you don't have to give it to the user permanently
- See the MPE/iX AIF:OS Reference Manual for details
  - http://docs.hp.com/mpeix/onlinedocs/36374-90013/36374-90013.html

```
AIFPROCGET(2119) /* obtain existing cap. mask */
set mask bit 21 for OP capability
AIFPROCPUT(2119) /* modify process cap. mask */
HPCICOMMAND("OP command string")
AIFPROCPUT(2119) /* restore original cap. mask */
```

Some read-only diagnostic tools require potentially destructive user capabilities

- :NETCONTROL requires CAP=NM
- :NSCONTROL requires CAP=NM
- NETTOOL.NET.SYS requires CAP=DI,NA,NM,PM
- These capabilities can cause havoc in the wrong hands!

:PURGEUSER and :PURGEACCT don't clean up creators or ACDs

- Results in files owned by users who no longer exist
- Results in ACDs granting access rights to users who no longer exist
- If you recreate one of these users, is it appropriate for that user to regain the old access rights?
- Third-party solutions exist for finding missing creators, but nothing for ACD problems
  - Scan :LISTFILE ,ACD every time you purge a user?

Anybody can do :LISTFILE @.@.@ to see all MPE-namespace files

- :LISTFILE exposes account names, group names, and file names even if you do not have access rights
- Descriptive names can be valuable information to a hacker
- Limit access to the CI prompt and the ability to execute CI commands
- HFS directories can be used in conjunction with POSIX security to prevent unauthorized users from viewing the contents below

Instead of :RELEASE, consider the use of ACDs (Access Control Definitions)

- :RELEASE is easy for getting around conventional file access restrictions, but tends to create huge security holes
- Instead use ACDs to grant different levels of access for different users of a file
- See :HELP ALTSEC for details
- For example:

```
:ALTSEC FDATA;NEWACD=(R:@.@; W,R:@.ACCT)
```

- Note: ACDs are the foundation for POSIX security

Networking

Null SNMP community name in SNMPSAMP

- SNMPSAMP.NET.SYS gives a null community name as an example to be used in SNMPCONF.NET.SYS
- Hackers know to try null or common community names such as "public"
- If using SNMP, choose a unique community name in SNMPCONF.NET.SYS
- SNMP queries can reveal lots of interesting information!
  - :XEQ SNMPWALK.NET.SYS localhost community

MPE TCP vulnerable to sequence number spoofing

- MPE TCP sequence numbers are predictable and can enable a hacker to impersonate your e3000 in order to exploit trust relationships
- For more info on TCP sequence spoofing, see: http://www.sans.org/rr/threats/intro_spoofing.php
- Patches are available to randomize MPE initial TCP sequence numbers:
  - 6.5: NSTGDV3 (LD)
  - 7.0: NSTGDV5 (GR)
  - 7.5: NSTGDW6 (LD)

Use external packet filtering

- MPE network transport lacks packet filtering
- Many MPE network services can allow or disallow by IP address, but this can be cumbersome to manage
- Use an external firewall or other network device to block all but explicitly authorized packets, I.e.:
  - port 23 (telnet)
  - port 80 (http)
  - port 1570 (vt)
  - source IP addresses from your intranet

Filter outbound ICMP timestamp & netmask replies

- MPE responds to ICMP timestamp & netmask requests
- A hacker who knows your local time could schedule attacks during the graveyard shift
- A hacker who knows your netmask is learning about your network topology
- Use an external firewall or other network device to filter these outbound ICMP replies from your e3000

Apache – allow or deny via IP address or hostname

- Module mod_access
  - http://httpd.apache.org/docs/mod/mod_access.html

```
order allow,deny
allow from 12.34.56.*
```

Apache – basic user/password authentication

- Module mod_auth
  - http://httpd.apache.org/docs/mod/mod_auth.html
- Web browser prompts for user & password which is authenticated against a simple Apache text file created by the htpasswd utility

```
AuthType Basic
AuthName "Restricted Directory"
AuthUserFile /path/to/htpasswd/file
Require valid-user
```

Apache – check logs for suspicious activity

- The /APACHE/PUB/logs/access_log file can indicate suspicious Microsoft IIS virus activity (Nimda, etc):

```
12.34.56.78 - - [20/Feb/2003:16:06:41 -0800] "GET
  /scripts/root.exe?/c+dir HTTP/1.0" 404 291
12.34.56.78 - - [20/Feb/2003:16:06:41 -0800] "GET
  /MSADC/root.exe?/c+dir HTTP/1.0" 404 289
12.34.56.78 - - [20/Feb/2003:16:06:42 -0800] "GET
  /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404
  299
12.34.56.78 - - [20/Feb/2003:16:06:42 -0800] "GET
  /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404
  299
```

WebWise – use HTTPS/SSL protocol for serving web pages

- https:// URLs use the Secure Sockets Layer (SSL) protocol to encrypt the data stream between the web browser and the web server
- If hackers should manage to network sniff this data stream, sensitive data will be protected
- If you are using unencrypted FTP to allow file downloads, consider switching to WebWise and encrypted https://
- http://www.modssl.org/docs/

WebWise – X.509 client authentication

- X.509 certificates aren't just for web servers!
- Require web browsers to submit valid X.509 certificates to be validated by the web server
  - http://www.modssl.org/docs/2.8/ssl_howto.html#ToC6
- Is the client certificate signed by the expected Certificate Authority?
- Does the client certificate contain the expected attributes?

WebWise - OpenSSL security functionality in FOS as part of the web server

- OpenSSL command line utility
  - file encryption/decryption
  - X.509 certificate management
  - S/MIME encrypted e-mail message generation
  - API libraries NOT included (but you can build them from source code from www.openssl.org)
- Only the X.509 functionality is supported, but the rest all works ☺
- 7.0: patch WBWGDT7A
- 7.5: included in mainline

FTP - log authentication attempts

- Recent versions of the MPE FTP server log the originating IP address for both successful and failed authentication attempts:
  - MPE 6.5: FTPGD01 or later
  - MPE 7.0: FTPGD49 or later
  - MPE 7.5: already in FOS
- See FTPDOC.ARPA.SYS for details

FTP - log authentication attempts (cont.)

```
11:04/#J5/138/FTP INVALID PASSWORD FOR:
  "HACKER,MANAGER.SYS" IP=12.34.56.78

11:04/#J5/138/FTP OPEN FOR:
  "SYSADMIN,MANAGER.SYS,PUB" IP=12.34.56.78
11:04/#J5/138/FTP CLOSE IP=12.34.56.78

11:07/#J5/147/FTP INVALID LOGON FOR:
  "BOGUS.ACCOUNT" IP=12.34.56.78
```

FTP – who is transferring what files?

- FTPSRVR doesn't explicitly log file transfer attempts
- But system logging file open & close events could be scanned to derive FTP usage

FTP - protocol logging would be helpful to detect certain hacking attempts

- Unfortunately FTPSRVR does not support protocol logging
- If access to FTPSRVR is controlled by an external firewall, proxy, or other network device, consider enabling FTP logging on the external device

FTP - restrict server usage to specific users

- MPE FTPSRVR is all or nothing – it cannot restrict access to certain users
- But Vesoft's Security/3000 product can

FTP - be aware of FTPSRVR's "site stream" command

- Allows remote users to stream batch jobs
- Users with CAP=BA,SF could upload new batch jobs to /tmp or other writable directories and then stream those jobs
- Defeats the use of "OPTION LOGON,NOBREAK" if such UDCs do not also restrict batch jobs
- A future version of FTPSRVR will likely add a new parameter to SETPARMS.ARPA.SYS to globally enable or disable "site stream"

FTP - don't enable anonymous FTP access

- Too many hacker tools scan for anonymous FTP access
- :PURGEUSER USER.FTPGUEST to make sure anonymous FTP is disabled (the default)
- Console messages for failed USER.FTPGUEST logons might indicate hacker scanning activity:

```
15:59/#J5/123/FTP INVALID LOGON FOR:
"USER.FTPGUEST,PUB" IP=12.34.56.78
```

INETD - Enable connection logging option (-l)

- The default mode is no logging
- Edit JINETD.NET.SYS and specify INFO='-l' to enable hostname and IP address information to be logged to JINETD $STDLIST for each INETD service connection attempt
- Note that DNS problems can *substantially* slow connection establishment

INETD - connection logging output

```
Received call for: ftp tcp
ftp/tcp: Connection from unknown
 (12.34.56.78) at Thu Feb 20 11:48:41 2003

Received call for: telnet tcp
telnet/tcp: Connection from some.host.name
 (87.65.43.21) at Thu Feb 20 15:58:24 2003

Received call for: ftp tcp
ftp/tcp: Connection from some.host.name
 (87.65.43.21) at Thu Feb 20 15:59:11 2003
```

INETD - disable unused services

- The INCNFSMP.NET.SYS template for the INETD config file INETDCNF.NET.SYS has many services enabled by default
- You should only enable those services that you are explicitly using
- Services like echo, daytime, time, discard, and chargen are not required by MPE
- Some of those services can be used in denial-of-service attacks

INETD – allow or deny via by IP address or hostname

- Use /usr/adm/inetd.sec to allow or deny access to INETD services by IP address or hostname
- Create /SYS/NET/INETDSEC from the INSECSMP sample file
- Make sure /usr/adm/inetd.sec is a symbolic link pointing to INETDSEC
  - ln –s /SYS/NET/INETDSEC /usr/adm/inetd.sec
- Controls all services listed in /etc/inetd.conf (aka /SYS/NET/INETDCNF)

Samba – encrypted passwords

- Samba/iX 2.0.7 and earlier only supported plaintext passwords
- Samba/iX 2.2.7a adds support for encrypted passwords
- Samba encrypted passwords are independent of MPE user & account passwords
  - stored in /usr/local/samba/private/smbpasswd
  - maintained with /usr/local/samba/bin/smbpasswd utility
- For more information: http://de.samba.org/samba/ftp/docs/htmldocs/ENCRYPTION.html

Samba – disable guest access

- Many hacking scanners attempt Samba guest access
- Modify /usr/local/samba/lib/smb.conf with "guest ok = no"

Samba – allow or deny via IP address or hostname

- In /usr/local/samba/lib/smb.conf:
- **hosts allow = 12.34.56.78**
- **hosts deny = badhost.somewhere.com**
- If a deny list conflicts with an allow list, the allow list takes precedence

Samba – check logs for suspicious activity

- Look for individual client log files in /usr/local/samba/var/log.*
- debug level = 2 needed to see failed authentication attempts (but also gives successful file open/close info)
- **log file = /usr/local/samba/var/log.%I** to log by client IP address instead of worthless client NetBIOS name

Sendmail – access database

- Accept or reject incoming e-mail

1. `:HELLO SERVER.SENDMAIL`
2. `:XEQ SH.HPBIN.SYS -L`
3.
```
shell/iX> /bin/cat - >/etc/mail/access
makemoneyfast@aol.com REJECT
imaspammer.com        REJECT
:EOD
```
4.
```
shell/iX> makemap hash /etc/mail/access
</etc/mail/access
```

- For further information, see: /SENDMAIL/CURRENT/cf/README

Sendmail – check syslog for suspicious activity

- Unauthorized relay attempts from spammers:

```
Oct 16 11:44:14 localhost sendmail[190251173]:
  f9GIi9M6190251173: ruleset=check_rcpt,
  arg1=<user@somewhere.com>, relay=spam.host.com
  [12.34.56.78], reject=550 5.7.1
  <user@somewhere.com>... Relaying denied
```

- Hacker probes:

```
Feb 20 16:26:10 localhost sendmail[1114264]:
  h1L0Q8ER1114264: hacker.host [12.34.56.78] did
  not issue MAIL/EXPN/VRFY/ETRN during connection
  to MTA
```

:STORE/:RESTORE

Untrusted OP users + :STORE-to-disk ;DIRECTORY is a bad combination

- OP users can :STORE ;DIRECTORY to obtain cleartext passwords
- Now that :STORE-to-disk is in FOS, physical access to tape media is no longer required
- Only give OP capability to those users who absolutely positively need it
- Purchase HP Security Monitor/iX and enable encrypted passwords

:RESTORE ;CREATE results in blank passwords

- If accounts, groups, or users get created by :RESTORE, they will have BLANK passwords
- Upon :RESTORE completion, remember to manually assign passwords to any newly created objects
- Periodically scan :LISTACCT/:LISTGROUP/:LISTUSER output for blank passwords

OP users can read or write any file using :STORE/:RESTORE

- Read the contents of any file
- Write arbitrary contents back to any file
- Think twice before giving OP capability to users!

Denial of Service

Configure sane connection limits

- Attackers can exhaust processor, memory, and disk resources by making hundreds (or thousands) of concurrent connections to network services
- Make sure each network service is configured with sane connection limits
  - :NMMGR global TCP and UDP parameters
  - :NSCONTROL SERVER=name,min,max
  - Apache MaxClients directive
  - Samba "max smbd processes" parameter
- Unfortunately no connection limits within INETD

Use Threshold Manager to define other limits

- Included in FOS for global management of resource utilization
- Only limits job & session logons, not process creations
- See Performing System Management Tasks manual for details

People & Processes

Help! I forgot my password!

- How can you be sure the user is who they say they are?
- What if you don't recognize their face or voice?
- Is a telephone request sufficient by itself?
- Is an e-mail request sufficient by itself?
- Should a handwritten signature be required?
- NEVER reveal an existing password – always change it to something new

Are your employee ID numbers secure?

- Social Security Numbers are too widely used for too many purposes to be truly secure
- Do internal corporate applications "leak" employee ID numbers to other unauthorized employees?

Terminate passwords when terminating employees

- Revoke or change passwords as soon as possible after the last day of employment
- But short of using mental telepathy, how do you know which passwords an employee knows?
- You may never know the full password list if informal password sharing is occurring
- Do you change EVERY password if you terminate the system manager?

Avoiding the phony security audit scam

- A hacker phones a user and says "Hi, Im from IT Support and Ineed to verify your password"
- Educate your users about what to expect and not expect from IT support staff
- Users should never reveal passwords to ANYBODY else!

Never share login accounts (or passwords)

- When multiple people share the same login account, reliable auditing becomes impossible
- Products like Vesoft's Security/3000 can help facilitate login sharing, but MPE system logging will not be aware of those extra levels of authentication

Beware of dumpster diving

- Implement procedures to prevent sensitive information being exposed in hardcopy trash
- Use caution when recycling – is the recycling facility secure?
- If in doubt, shred!

Control access to used backup media

- System backups contain passwords and other sensitive information
- Who has physical access to on-site media?
- Who can request media from off-site archives?
- When used media cycles back into the scratch pool, do you zero-out the old data before making the media available for reuse?

Knowledge retention

- Employees with MPE OS & local application skills may leave to seek a different career path
- Will the employees who are left have sufficient skills to ensure good MPE & application security?
- Make sure critical knowledge is written down somewhere

Keep current on software versions

- Perform periodic OS & application software updating/patching to get fixes for security problems
- MUCH Internet grief could be prevented if everybody was up-to-date on key software
- For MPE patches, the unsupported freeware patchman utility can help
  - http://www.bixby.org/ftp/pub/mpe/patchman-2.2.sh

Stay informed

- Subscribe to vendor security alert mailing lists
- Subscribe to Internet security alert mailing lists such as CERT, CIAC, BUGTRAQ, etc
- Subscribe to open source application "announce" lists
- Subscribe to open source application developer lists
- Subscribe to HP3000-L/comp.sys.hp.mpe
- What you don't know CAN hurt you!

The future

MPE security 2003-2006: the good news

- HP software support continues through 2006
- HP software delivery continues through 2006
- HP patches continue through 2006
- In short, nothing has changed from a customer support perspective

MPE security 2003-2006: the bad news

- MPE 6.0 and earlier already not supported by HP
- MPE 6.5 end of HP support date 12/31/04
- MPE 7.0 end of HP support date 12/31/06
- MPE 7.5 end of HP support date 12/31/06
- No HP patches for security or other problems after these dates!

MPE security beyond 2006 – native bugs

- Vastly fewer customers using MPE means some undiscovered native security problems may stay hidden
  - good news: fewer MPE-specific security problems will emerge
  - bad news: if problems do emerge, HP won't be willing to fix them
- Third-party support providers may be willing and able to provide fixes for some new bugs

MPE security beyond 2006 – open source bugs

- Internet hackers will continue to find bugs in the open source products which are bundled into MPE
  - Apache, BIND, Samba, Sendmail
- Most of these bugs tend to be of the buffer overflow / code execution variety, which at most will cause a process abort on MPE without executing any hacker code
- HP will no longer be providing updated open source binaries for MPE
- If these products are critical for your homesteading environment, you should invest in learning some Unix to MPE porting skills so you can update the products yourself (it's not that difficult!)

Real-life security stories from the audience

General Q&A


hp
invent