

Macintosh OS X Security Issues

Matthew Cook
Loughborough University
<http://escarpment.net/>

RSC East Midlands



Introduction

- Overview of Macintosh Security Issues
- Anti Virus
- Password Protection
- Operating System Patching
- Sharing Services

- Machine Compromise - Forensics

But we own a Macintosh?

For a long time security was not a major issue with the Macintosh platform:

- Security through obscurity
- Well written Operating System
- Poor IP Stack

Time has not stood still...

Today's Macintosh

- Operating System based on UNIX/BSD
- Faster connection speeds
- Widening user base
- More security aware information age

- Do we still need to worry?

Security Issues

- In 2005, so far, 11 Security Issues
- One remains un-patched
- None highly critical, 36% Important
- 64% Remote Exploit, 36% Local
- 16% Resulted in System Access

- Source: Secunia

...and compared with Windows?

- 15 Security Issues
- Four remain un-patched
- 33% Highly Critical, 33% Important
- 67% Remote Exploit, 23% Local
- 56% Resulted in System Access

- Source: Secunia
Based on Windows XP Professional

However...

There are steps to ensure your Macintosh machine is secure:

- Install Anti Virus software.
- Password Protection
- Install Operating System Patches.
 - Software Updater
 - Application Updates
- Do NOT use Peer to Peer networks or software from suspect sources.

Anti Virus Software

- No Anti Virus Software leaves your machine open to virus infection!
- You transfer viruses to Macintosh and Windows users alike!
- You risk losing data with examples like the Word Macro Virus!
- Any Anti Virus software is useless without updated DAT files.

Password Protection

- Ensure your machine is Password Protected.
- The use of Auto-login is not recommended.
- Ensure Screen Savers are password protected.

Operating System Patches

- Essential to ensure the machine is secured.
- Use Apple's Software Update utility to keep your machine updated.
- Unfortunately no equivalent to SUS, WSUS or SMS. Radmin is a possibility?
- Other Applications need patching too!

If you don't patch?

- Root shell in four steps? (<10.20.2001)
2. Open up the Terminal.app
 3. Quit it.
 4. Open up NetInfo Manager (leave it in the foreground)
 5. Open up Terminal.app from the *RECENT ITEMS* list in the Apple Menu.

Sharing

- System Preferences -> Sharing
 - Personal File Sharing
 - Windows Sharing
 - Personal Web Sharing
 - Remote Login
 - FTP Access
 - Apple Remote Desktop
 - Remote Apple Events
 - Printer Sharing

Overview Conclusions

- You need to take action, you can't be complacent
- Install Anti-Virus Software
- Patch your Operating System
- Patch Applications
- Only enable necessary services
- Secure with suitable passwords

Machine Compromise

Macintosh OS X Forensics

Initial Activity

Saturday 29th January:

- Strange patterns of UDP port 53 traffic
- From University host to the Internet
- MAC address filter placed on the switch port feeding the unmanaged equipment feeding the host.

Nmap Scan

```
# nmap -A -O -p0-65535 158.125.x.x
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-01-28 23:26
GMT
Interesting ports on cm-x-x.lut.ac.uk (158.125.x.x):
(The 65529 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE      VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp
22/tcp    open  ssh          OpenSSH 3.4p1+CAN-2004-0175 (protocol 1.99)
139/tcp   open  netbios-ssn Samba smbd (workgroup: WORKGROUP)
427/tcp   open  svrloc       Apple sldap
548/tcp   open  afp          Apple AFP (name: Organic; protocol 3.1; Mac OS
X 10.2
Device type: general purpose
Running: Apple Mac OS X 10.1.X|10.2.X
OS details: Apple Mac OS X 10.1 - 10.1.4, Apple Mac OS X 10.1.5-10.2.8
```

Tcpdump

```
# tcpdump -X -eqntl -i eth3 host 158.125.x.x

00:d0:03:86:c4:00 > 00:07:0d:22:1c:0a, IPv4, length 60: IP
158.125.x.x.51113 > 130.243.33.230.domain: UDP, length 15
 0x0000: 4500 002b 57f8 0000 3f11 4dd5 9e7d 929e E..+W...?.M..).
 0x0010: 82f3 21e6 c7a9 0035 0017 935b 3031 3233 ..!....5...[0123
 0x0020: 3435 3637 3839 4142 4344 4555 5555
456789ABCDEUUU
00:d0:03:86:c4:00 > 00:07:0d:22:1c:0a, IPv4, length 60: IP
158.125.x.x.51113 > 130.243.33.230.domain: UDP, length 15
 0x0000: 4500 002b 5809 0000 3f11 4dc4 9e7d 929e E..+X...?.M..).
 0x0010: 82f3 21e6 c7a9 0035 0017 935b 3031 3233 ..!....5...[0123
 0x0020: 3435 3637 3839 4142 4344 4555 5555
456789ABCDEUUU
```

Tcpdump (disconnection)

```
# tcpdump -eqntl -i eth3 host 158.125.x.x

00:07:0d:22:1c:0a > 00:d0:03:86:c4:00, IPv4, length 74: IP
80.97.37.139.2194 > 158.125.x.x.ssh: tcp 20
00:07:0d:22:1c:0a > 00:d0:03:86:c4:00, IPv4, length 74: IP
80.97.37.139.2194 > 158.125.x.x.ssh: tcp 20
00:07:0d:22:1c:0a > 00:d0:03:86:c4:00, IPv4, length 114: IP
80.97.37.139.2194 > 158.125.x.x.ssh: tcp 60
00:07:0d:22:1c:0a > 00:d0:03:86:c4:00, IPv4, length 114: IP
80.97.37.139.2194 > 158.125.x.x.ssh: tcp 60
00:07:0d:22:1c:0a > 00:d0:03:86:c4:00, IPv4, length 254: IP
80.97.37.139.2194 > 158.125.x.x.ssh: tcp 200
00:07:0d:22:1c:0a > 00:d0:03:86:c4:00, IPv4, length 62: IP
80.97.37.139.2521 > 158.125.x.x.ssh: tcp 0
```

The Next Working Day

Monday 31st January:

- Confirmed the machine was an iMac running Macintosh OS X 10.2.8
- Machine was removed from the network for investigation
- Macintosh security advice was sought

The Investigation

- Carried out on local machine
- Better ways of doing things...
 - Forensic Tool Kit
 - Disc Image
 - Read only hard disc
 - Actual hard disc
- More experience and time required

Getting Root

- Logged into the machine as an administrative user.
- Created a root account.
 - Using NetInfo Manager
 - /Applications/Utilities/NetInfo Manager
 - Domain -> Security -> Authenticate
 - Domain -> Security -> Enable Root User

System Information

```
# uname -a
```

```
Darwin cm-x-x.lut.ac.uk 6.8 Darwin Kernel Version 6.8: Wed  
Sep 10 15:20:55 PDT 2003; root:xnu/xnu344.49.obj-2/  
RELEASE_PPC Power Macintosh powerpc
```

Patches Outstanding:

Security Update 2005-001 1.0 17.9MB

- ColorSync
- PHP
- Safari

System Logs

```
# grep -i sshd /private/var/log/system.log*
```

```
system.log:Jan 31 08:58:58 iMac sshd[326]: Server listening on  
0.0.0.0 port 22.
```

```
system.log:Jan 31 09:00:16 iMac sshd[326]: Received signal  
15;terminating.
```

```
system.log.0:Jan 29 21:17:54 iMac sshd[1924]: Failed password for  
mike from 80.97.37.139 port 2194
```

```
system.log.0:Jan 29 21:17:57 iMac sshd[1924]: Accepted password  
for mike from 80.97.37.139 port 2194
```

```
system.log.0:Jan 29 23:20:18 iMac3 sshd[1992]: Bad protocol  
version identification " from 158.125.x.x
```

```
system.log.7:Jan 23 00:41:07 iMac sshd[841]: Could not reverse  
map address 203.239.145.5.
```

```
system.log.7:Jan 23 00:41:07 iMac sshd[841]: Failed password for  
root from 203.239.145.5 port 52398 ssh2
```

FTP Logs

```
# cat /private/var/log/ftp.log*
```

```
Jan 22 14:59:40 iMac ftpd[748]: connection from  
tra42-1-82-232-180-30.fbx.proxad.net to cm-x-x.lut.ac.uk
```

```
Jan 28 20:19:47 iMac ftpd[1681]: connection from
```

```
fontenay-4-81-56-43-71.fbx.proxad.net to cm-x-x.lut.ac.uk
```

```
Jan 12 13:50:33 iMac ftpd[3589]: connection from  
host14-80.pool80181.interbusiness.it to cm-x-x.lut.ac.uk
```

```
Jan 6 03:42:32 iMac ftpd[1086]: connection from
```

```
cab-193230.calixo.net to cm-x-x.lut.ac.uk
```

Last

```
# last
mike ttyp0 matrix09.matrixv Sat Jan 29 21:17 - 23:34 (02:16)
mike ttyp0 matrix02.matrixv Fri Jan 28 21:47 - 22:05 (00:17)
mike ttyp0 itms.rutgers.edu Fri Jan 28 21:12 - 21:20 (00:08)
mike ttyp0 h169-210-68-8.ad Wed Jan 26 01:01 - 01:01
(00:00)
mike ttyp0 217.222.184.110 Sun Jan 23 03:48 - 03:48 (00:00)
mike ttyp0 217.222.184.110 Sat Jan 15 07:10 - 07:10 (00:00)
mike ttyp0 ns.c-line.ru Sat Jan 15 05:59 - 06:10 (00:10)
```

Password File

```
# cat /etc/passwd
nobody:*:-2:-2:Unprivileged User:/nohome:/noshell
root:*:0:0:System Administrator:/var/root:/bin/tcsh
daemon:*:1:1:System Services:/var/root:/noshell
smmsp:*:25:25:Sendmail User:/private/etc/mail:/noshell
www:*:70:70:World Wide Web Server:/Library/WebServer:/noshell
mysql:*:74:74:MySQL Server:/nohome:/noshell
sshd:*:75:75:sshd Privilege separation:/var/empty:/noshell
unknown:*:99:99:Unknown User:/nohome:/noshell
```

Group File

```
# cat /etc/group
nobody:*:-2:
nogroup:*:-1:
wheel:*:0:root
daemon:*:1:root
kmem:*:2:root
sys:*:3:root
tty:*:4:root
operator:*:5:root
mail:*:6:
bin:*:7:
staff:*:20:root
smmsp:*:25:
guest:*:31:root
utmp:*:45:
uucp:*:66:
dialer:*:68:
network:*:69:
www:*:70:
mysql:*:74:
sshd:*:75:
admin:*:80:root
unknown:*:99:
```

Nidump – Password File

```
# nidump passwd .

nobody:*:-2:-2::0:0:Unprivileged User:/dev/null:/dev/null
root:Ydz/bbYwtuVXs:0:0:0:0:System
Administrator:/var/root:/bin/tcsh
daemon:*:1:1:0:0:System Services:/var/root:/dev/null
unknown:*:99:99:0:0:Unknown User:/dev/null:/dev/null
www:*:70:70:0:0:World Wide Web
Server:/Library/WebServer:/dev/null
<SNIP>
mike:z6i8B7h2Mz2Ao:562:20:0:0: <Names> /Users/mike:/bin/tcsh
```

Nidump - Group File

```
# nidump group .

nobody:*:-2:
nogroup:*:-1:
wheel:*:0:<root users>
daemon:*:1:root
kmem:*:2:root
sys:*:3:root
tty:*:4:root
operator:*:5:root
mail:*:6:
bin:*:7:

staff:*:20:root
guest:*:31:root
utmp:*:45:
uucp:*:66:
dialer:*:68:
network:*:69:
www:*:70:
admin:*:80:<root users>
unknown:*:99:
smmisp:*:25:
mysql:*:74:
sshd:*:75:
```

Lsof - Netstat

```
# lsof
Shows the Processes running, the PID,
user and location on filesystem

# netstat -a
Shows active network connections, IP
addresses and ports.
```

Bash_history

```
# cat /Users/mike/.bash_history
export PATH=.:$PATH
x
s
chmod +x s
s
ls
chmod +x x
x
clear
s 131.111.144.236 53
s 83.243.47.2 22
```

Hidden Files

```
# locate " ."
/private/var/tmp/ ./s
/private/var/tmp/ ./x

Could/should have used 'find'...
```

DoS Attack Tools

```
# cat "/private/var/tmp/ ./x"

#!/usr/bin/perl
#####
# udp flood.
#
# gr33ts: meth, etech, skrilla, datawar, fr3aky, etc.
#
# --/odix
#####

# strings "/private/var/tmp/ ./s"

8_PAGEZERO
H_TEXT
```

S Disassembly

- # otool -v -t s
 - Usage: st-kill <host> <port>
 - "This tool is extremely dangerous. Use at your own risk!"
 - Just sends 'BOMB_STRING' to host and port with no time delays
 - No <secs> argument
 - <http://lists.netsys.com/pipermail/full-disclosure/2002-August/001084.html>

Weak Passwords

- L0phtcrack & John the Ripper:
 - bex swimming 0d 0h 0m 18s
 - curley pistol 0h 0m 14s
 - f402 organic 0d 0h 0m 13s
 - jonshotton help 0d 0h 0m 9s
 - olivier olivier 0d 0h 0m 0s
 - root recovery 0d 0h 0m 15s
 - sweta guitar 0d 0h 0m 8s
 - vincent dragon 0d 0h 0m 6s

In Summary

- The user mike had a weak password
- The user mike had admin rights
- Automated login attempts succeeded
- The cracker uploaded files to a more obscure area of the file system
- The cracker logged in from other hosts
- Attacks were made on other systems

SSH Versions

```
telnet 127.0.0.1 22
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
SSH-1.99-OpenSSH_3.6.1p1+CAN-2004-0175
```

```
telnet 127.0.0.1 22
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
SSH-1.99-OpenSSH_3.4p1
```

Mac Security Links

- <http://www.lboro.ac.uk/computing/security/>
- <http://www.apple.com/support/security/>
- <http://www.securemac.com/>
- <http://members.lycos.co.uk/hardapple/>
- <http://www.macsecurity.org/>

Questions?

<http://escarpment.net/>
