

---

# Apple Security Concerns

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

# Introduction

---

- Overview of Macintosh Security Issues
- Anti Virus Software
- Malware Issues
- Password Protection
- Operating System Patching
- Bad Installers
- Sharing Services
- AFP Security
- 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
- Mac OS X for Intel
- More security aware information age
- Do we still need to worry?

# Default Macintosh

---

- Nothing listening by default.
- Therefore not remotely exploitable.
- Also its biggest advantage, unlike; Windows, Solaris and most other Operating Systems.
- Local exploits are a different matter!

# Security Issues

---

- In 2005, so far, 20 Security Issues
- None remain un-patched
- 36% Highly Critical, 34% Moderate
- 78% Remote Exploit, 22% Local
- 20% Resulted in System Access
  
- Source: Secunia

# ...and compared with Windows?

---

- 43 Security Issues
- Eight remain un-patched
- 33% Highly Critical, 32% Moderate
- 82% Remote Exploit, 18% Local
- 50% Resulted in System Access
- Source: Secunia (Windows XP Pro)

# 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!
- *However Dom will discuss this issue in greater detail later...*

# Malware Issues

---

- Ad/Spy/Malware – Are they a problem?
- No is the common misconception!
- Tracking Cookies
- Office related vulnerabilities
- Rootkits; Opener, osxrk, Togroot and WeaponX
- It is only time before there is a serious threat to Mac OS X!

# 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.
- Other Applications need patching too!
- Microsoft Office updates are provided by a separate application.

# Operating System Patches

---

- Unfortunately no equivalent to SUS, WSUS or SMS.
- Radmin or Casper is a possibility.
- Altiris is soon to have Mac OS X Support included.

# If you don't patch?

---

Root shell in four steps? (<10.20.2001)

1. Open up the Terminal.app
2. Quit it.
3. Open up NetInfo Manager (leave it in the foreground)
4. Open up Terminal.app from the \*RECENT ITEMS\* list in the Apple Menu.

# More recently?

---

- System preferences Root Exploit for 10.3.6.
- Add admin users, enable root.
- Even works over SSH connection.
- Very simple AppleScript.
- Another reason why patching is critical!

# Bad Installers

---

- /Library/StartupItems
- Why is that important? Ran as root!
- Badly coded installers creating their directory with the incorrect permissions.
- Apple Disk Utility does repair permissions.
- This is not just a Mac OS X issue.

# Sharing Services

---

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

# AFP Security

---

- Currently AFP traffic is not encrypted.
- Passwords could be clear text.
- Worse than SMB!
- User Authentication Methods
  - ClearText
  - Random Number Exchange (Two Way)
  - Diffie-Hellman Exchange (2)
  - Kerberos

# AFP Security...

---

- 10.3 and 10.4 Server support native AFP over SSH.

- Otherwise:

```
ssh -L 10548:127.0.0.1:548 user@server  
afp://127.0.0.1:10548/
```

# 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

---

Full forensics provided at Networkshop 33

<http://www.ja.net/services/events/calendar/2005/networkshop-33/mattcook.pdf>

An excellent event for technical knowledge sharing in both HE and FE.

# Machine Compromise...

---

## Useful Tools/Commands

- Nmap -A -O -p0-65535 <host>
- Tcpdump -X -eqntl -I eth0 host <host>
- /private/var/log/system.log\*
- /private/var/log/ftp.log\*
- last
- /etc/passwd, /etc/shadow and /etc/group
- nidump passwd . Or nidump group .

# Machine Compromise...

---

- lsof
- netstat -a
- <user>/.bash\_history
- locate or find “.”
  
- SSH security
- telnet 127.0.0.1 22

# 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/>