

---

# **Macintosh OS X Security, should we worry?**

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



S S S S S S S F

S S S S S S S 3

# Introduction

---

- Thank you Dom for inviting me to this Technical Forum.
- The Security Service has been running for approximately just one year.
- In this time NO Macintosh machines have been found compromised.
- Although several incidents of Viruses and AUP abuse.

# Why do we need security?

---

- Denial of Service
- Theft of information
- Modification
- Fabrication (Spoofing or Masquerading)
- Bringing the institution into disrepute
- Spreading infection
- ...More unnecessary work

# 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
- Well written applications

Time has not stood still...

# Today's Macintosh

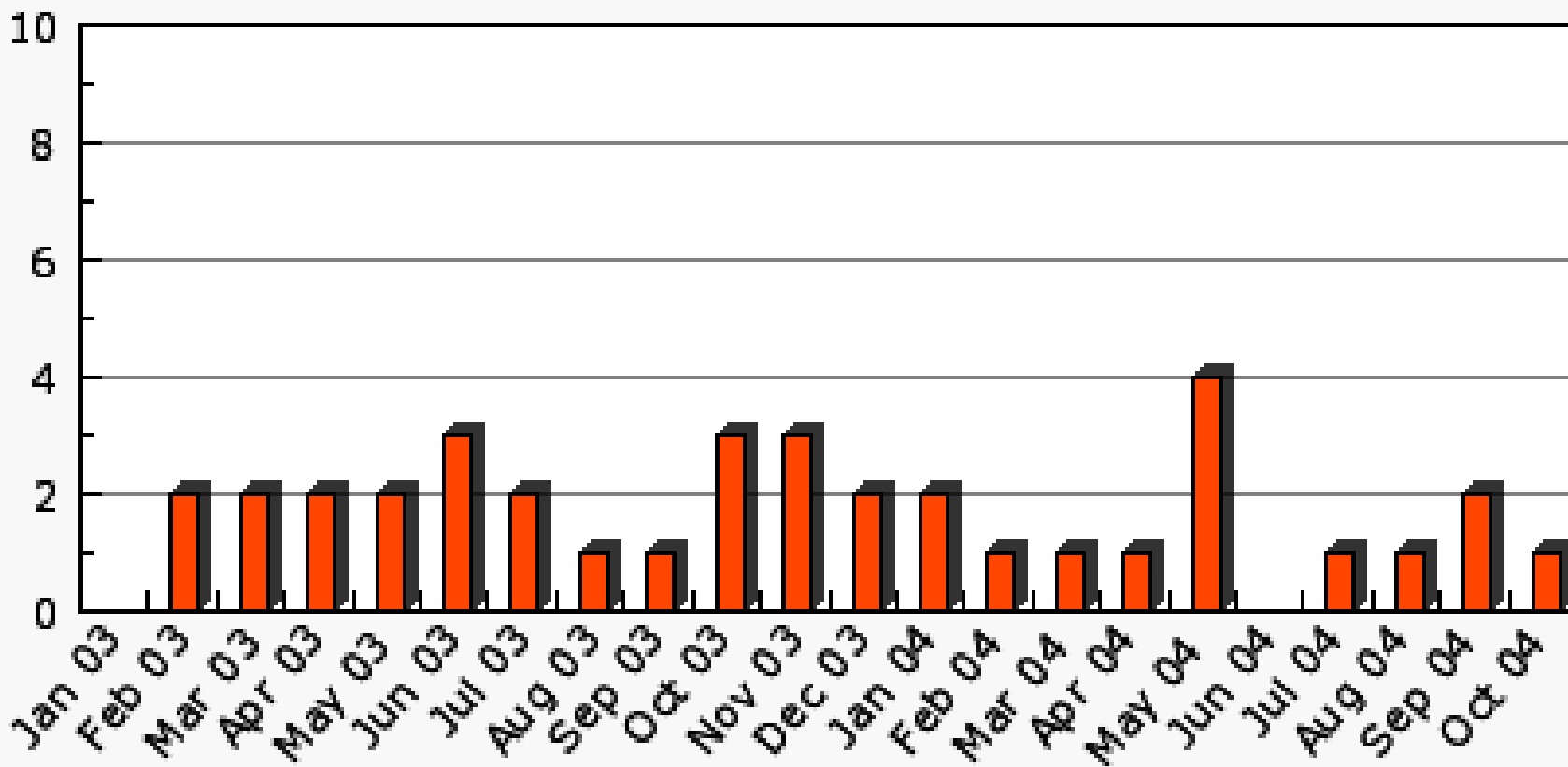
---

- Operating System based on UNIX
- Faster connection speeds
- Widening user base
- More security aware information age
- Do we still need to worry?

# Frequency of Advisories

## Apple Macintosh OS X

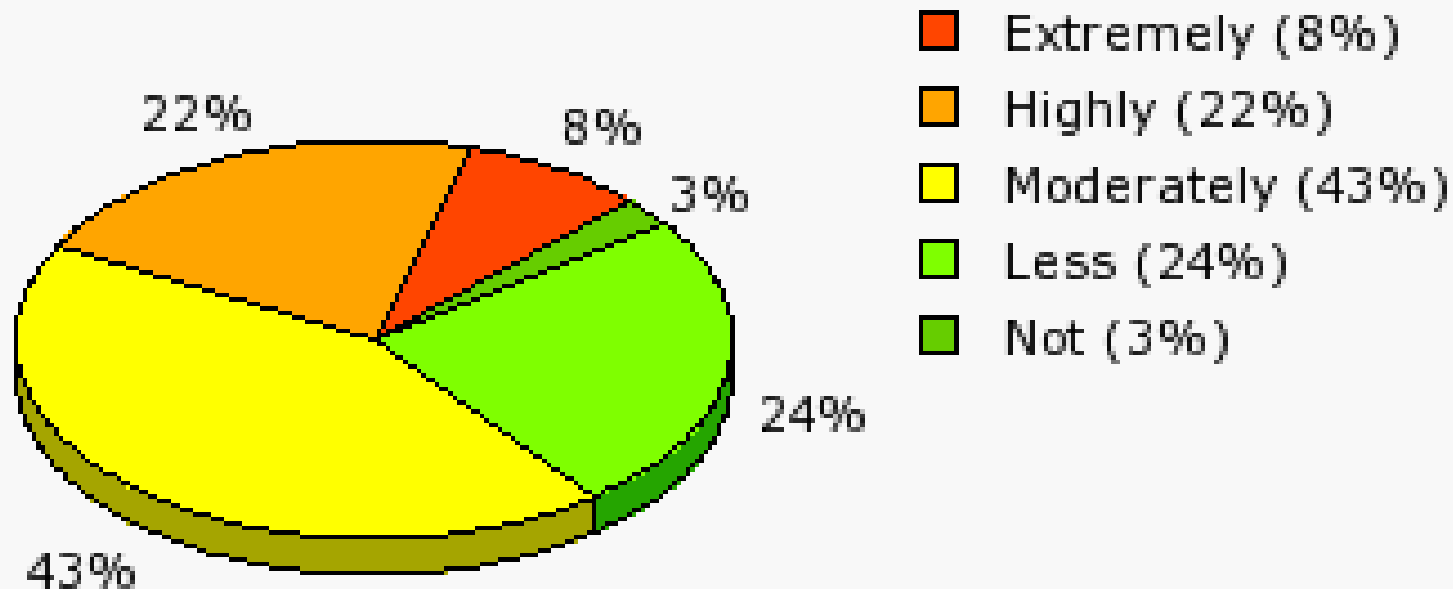
Advisories (Based on 37 advisories from 2003-2004)



This graph was generated by Secunia.

# How Critical?

## Apple Macintosh OS X Criticality (Based on 37 advisories from 2003-2004)



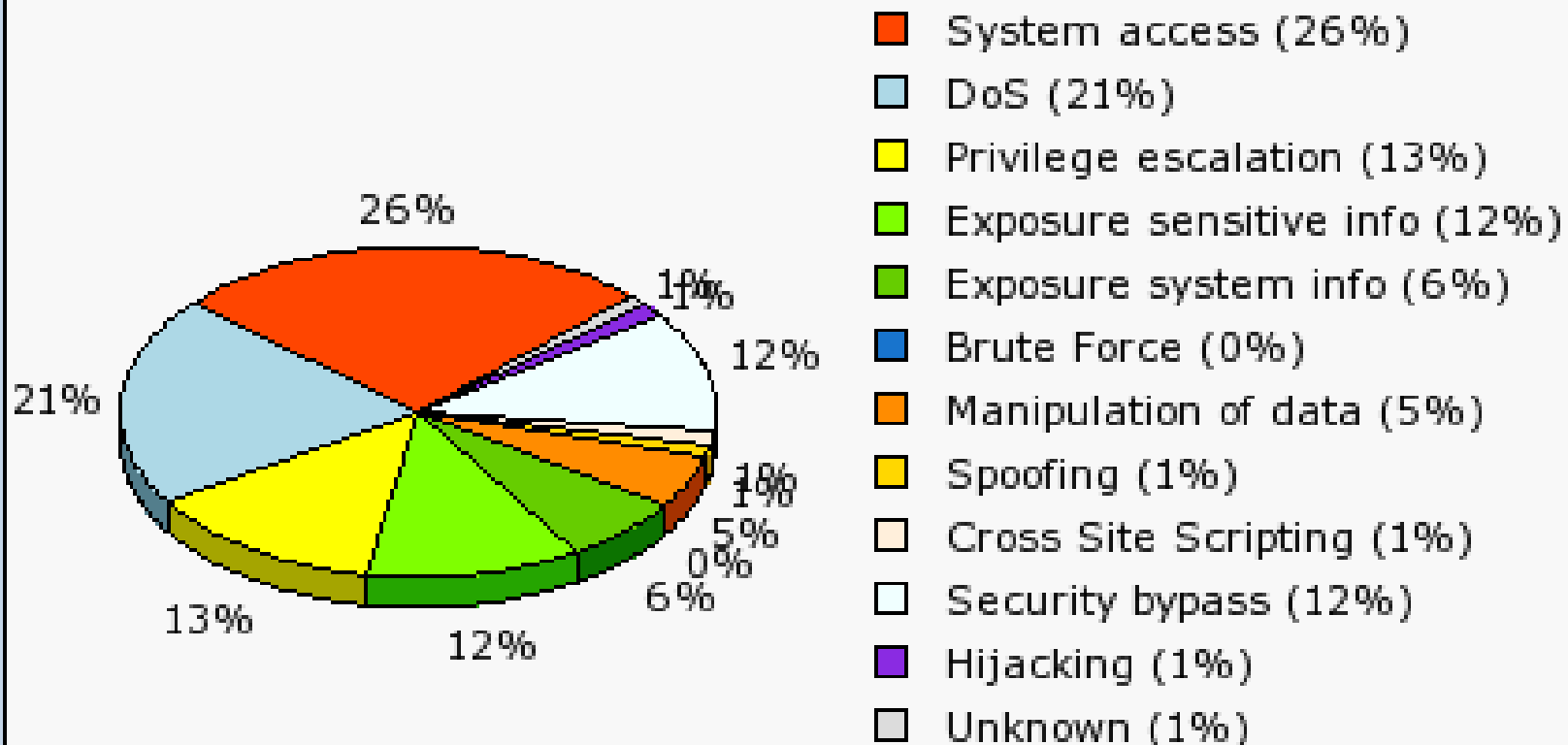
This graph was generated by Secunia.

Based on Secunia Advisories freely available at <http://secunia.com/>

# Impact of the advisory

## Apple Macintosh OS X

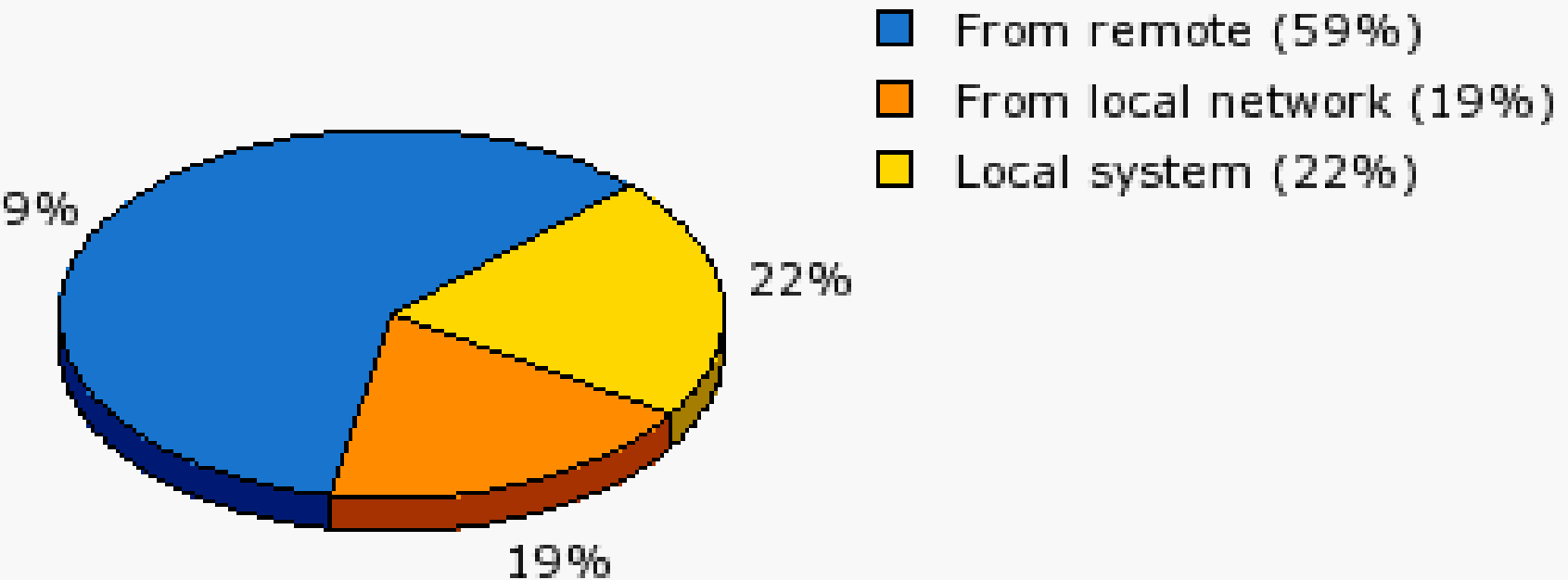
Impact (Based on 37 advisories from 2003-2004)



# Attack Vector

## Apple Macintosh OS X

Where (Based on 37 advisories from 2003-2004)



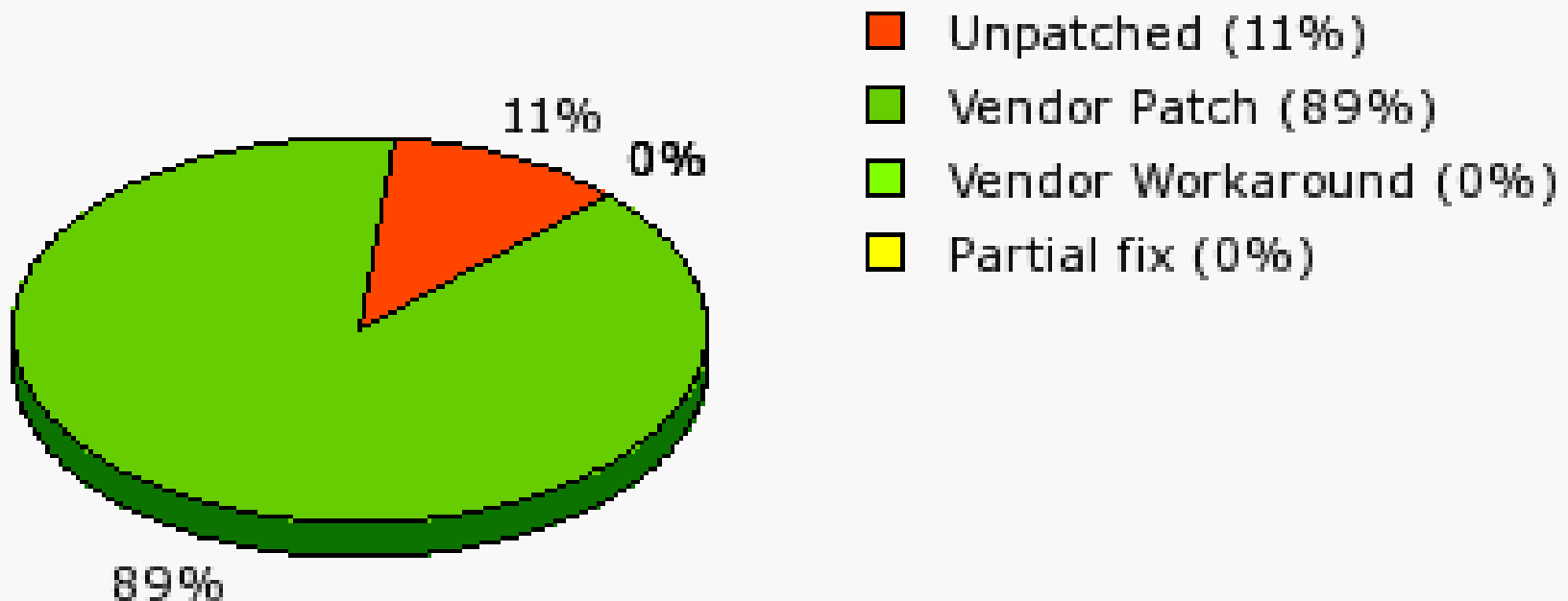
This graph was generated by Secunia.

Based on Secunia Advisories freely available at <http://secunia.com/>

# Solution Status

## Apple Macintosh OS X

Solution Status (Based on 37 advisories from 2003-2006)



This graph was generated by Secunia.

Based on Secunia Advisories freely available at <http://secunia.com/>

# Un-patched Vulnerabilities

---

- Apple Mac OS X Internet Connection Privilege Escalation (27/07/2004)
- Apple Filing Protocol Insecure Implementation (01/03/2004)
- Mac OS X Local Denial of Service Vulnerability (05/01/2004)
- Mac OS X Screen Lock Bypass Vulnerability (29/10/2003)
- Mac OS X Local root (13/09/2002)

# ...and compared with Windows?

---

- In 2003/04 Mac OS X had the largest share of 'extremely critical' advisories at 19%
- 37 advisories for Mac OS X compared to 46 for Windows XP Professional

Statistics won't make you buy a Windows machine, nor will I recommend you do!  
The best tool for the job is needed.

# However...

---

There are steps to ensure your Macintosh machine is secure:

- Install Anti Virus software.
- Password Protection
- Install Operating System Patches.
- Do NOT use Peer to Peer networks or software from suspect sources.
- Join the University Macintosh mailing lists.

# Anti Virus Software

---

- The AUP states all machines connected to the campus network must have Anti Virus Software installed.
- The University has a license for Virex 7.
- Any Anti Virus software is useless without updated DAT files.

<http://www.lboro.ac.uk/computing/virex.html>

# Password Protection

---

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

# If you don't install?

---

- You are breaking the University AUP!
- You leave 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!

# Operating System Patches

---

- Essential to ensure the machine is secured.
- Use Apple's Software Update utility to keep your machine updated.
- Read the University Macintosh mailing lists to keep up to date.
- Test patches before installing or check with other users on campus first!

# 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.

# Conclusions

---

- You need to take action, you can't be complacent
- Ensure YOU protect the campus network infrastructure
- Install Anti-Virus Software
- Patch your Operating System
- Join the mailing lists

# Resources

---

maxmac@lists.lboro.ac.uk

mac-security@lists.lboro.ac.uk

<http://www.lboro.ac.uk/computing/security/>

<http://www.apple.com/support/security/>

<http://secunia.com/vendor/17/>

<http://www.securemac.com/>

---

# Questions?

<http://escarpment.net/>