

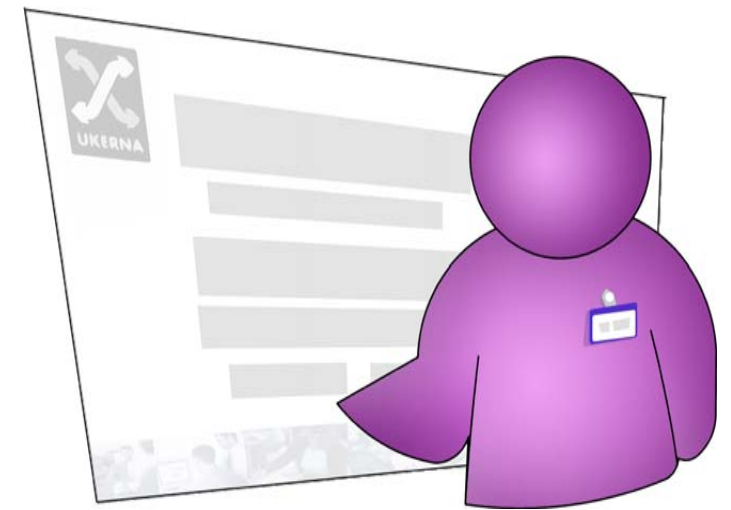
# Practical Apple Mac Security Recommendation





# Introduction

- Matthew Cook
- Senior IT Security Specialist  
(Loughborough University)
- UKERNA Contracted Trainer
- Further details available at:  
<http://escarpment.net/>



# Background

- Why are we here?
- For a long time security was not a major problem on the platform
- Security through obscurity
- Well written Operating System
- Poor IP Stack
  
- Time has not stood still...

# The Macintosh of Today

- Operating System based on UNIX/BSD
- Widening User Base
- Mac OS X for Intel
- Security aware information age
- Number of threats increasing
- Popular software ported
  
- Still no need to worry?



# Default Macintosh

- Out of the box
  - Nothing listening by default
  - Difficult to compromise
  - A very big advantage
- 
- Local exploits are a different matter!



# Local Exploits

- A big problem
- A locked down machine, becomes...
- Fully patched 10.4.8
- Bill of Materials
- /Library/Receipts
- Processing BOM files via diskutil

# Anti Virus Software

- Still essential
- There are Macintosh viruses
- Acting as a carrier
- Loosing data, Word Macro Virus
  
- Currently around 50 specific threats, but growing.

# 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.
- No equivalent to WSUS or SMS
- Radmin, Casper or Altiris?



# 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



# Steps to Security

- 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



# UKERNA Training

- Portfolio of network based training
- Over 10 different courses
- Training venues in many locations
- Comprehensive course workbook + CD
  
- Using Logfiles for Security
- Basic Networking
- Wireless LAN Fundamentals
- Firewalls: Planning and Implementation

# Questions?

<http://escarpment.net/>