Mac OS X Client Lab Security

Part 1

James Reynolds
Student Computing Labs
The University of Utah

What Is Lab Security?

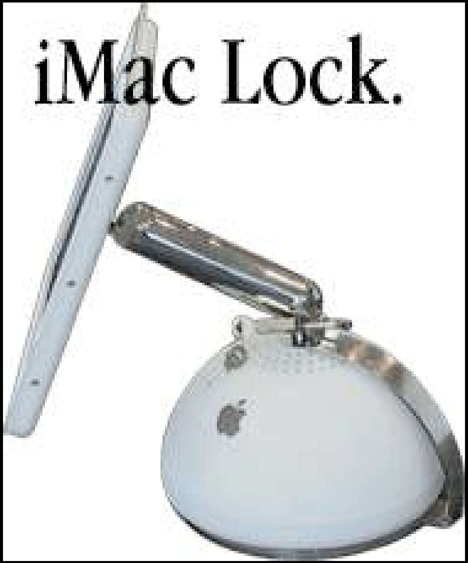
Controlling usage

- Why
  - Preserve privacy
  - Stop malicious behavior
- How
  - Permissions
  - Automated monitoring

Physical Security

Lock the CPU

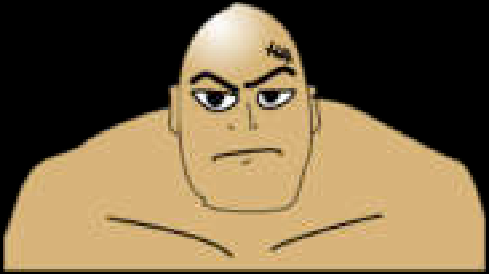
- Use thick cables or chains
- Use special locks or screws for iMacs



Physical Security

Lab Environment

- Cameras
- Alarms
- Attentive staff
- Card reader



Physical Security

Monitor tampering

- Network monitoring
    - InterMapper
    - Nagios

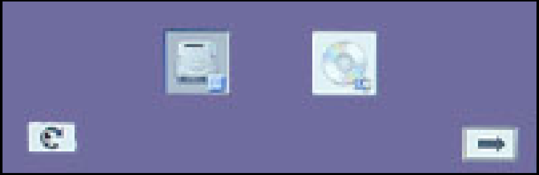
Automated system profiling

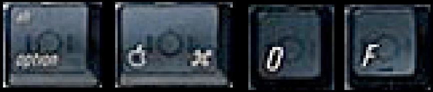
- Apple Remote Desktop
- InterMapper
- “system_profiler”

Boot Security

What is boot security?

- Bypass ALL security: boot to a different hard disk
- Mac OS X offers many ways to do this

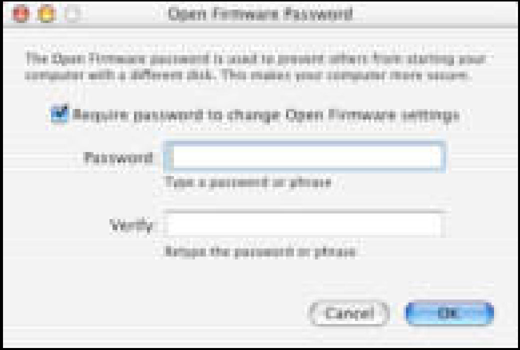




Boot Security

Open Firmware

- What is it?
- Set it
  - Apple’s tool
  - OFPW tool
- Verify
  - Is it set?
  - Is it correct?



Open Firmware Password

The Open Firmware password is used to prevent others from starting your computer with a different disk. This makes your computer more secure.

☑ Require password to change Open Firmware settings

Password

Type a password or phrase

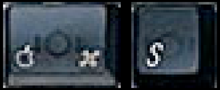
Verify

Retype the password or phrase

Boot Security

Older hardware

- Single user mode
  - SecureIt

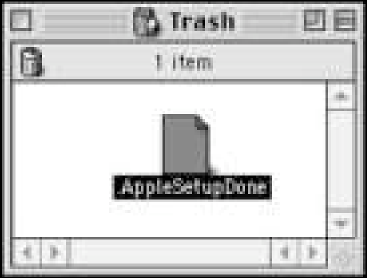


- Drives
  - Unplug CD, ZIP, Floppy drives
  - Do not install Classic
  - Use only one hard disk partition
  - Beware external drives (SCSI, etc)

Boot Security

Mac OS 9/Classic

- DO NOT dual boot
- Lock Startup Disk prefs
- Use shadow disk image
  - ShadowClassic



Regular Hard Disk Cleanup

File by file cleanup

- Radmind
- RsyncX

Imaging

- Apple Software Restore

Tripwires

- Radmind
- CheckMate
- Tripwire

Published Exploits

Push out updates ASAP

- Radmind
- RsyncX
- ASR

Stay informed by staying involved

- Apple’s security list
- Many other lists
  - Small lists are often the 1st to know

Admin System Changes

Code wisely

- Every modification a potential hole
- Use full paths
- Use trusted system calls/tools

Permissions

- Check, check, check, check

Admin System Changes

Remove access

- Remove world read permissions
    - Cron
    - Startup Items
    - LoginHook and LogoutHook
- Set allow list for cron execution
- Do not enable root user

World Writable

Protect non-user file space

- Setup image carefully!
  - Track OS & software installs
    - Radmind or File Buddy
  - Remove world write permissions
    - Not Caches, ColorSync Profiles, User space, /.Trashes, /Volumes, /cores, /dev, /tmp, /var/run, and /var/tmp

World Writable

Use links/aliases/disk images for:

- Final Cut Pro
- Omnipage Pro
- Painter
- Now Up To Date
- Virtual PC
- FreeHand
- Classic QuarkXPress 4.11

World Writable

Find world writable

- WhoOwnsWhat
- “sudo find / -perm -2”

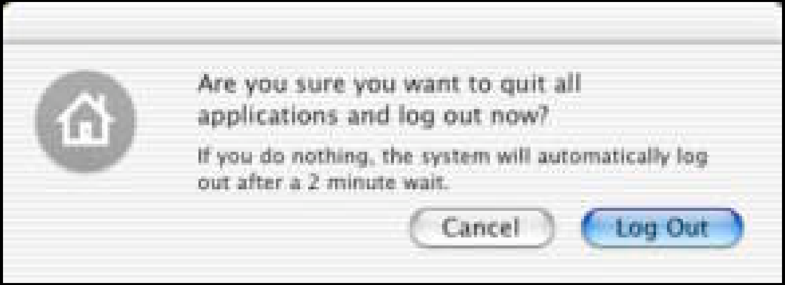
Check writable at startup

- Automate “find <path> -perm 2”

After Logout - “nohup”

What is it?

- No hangup
  - nohup <command>
- Does not quit at logout



Are you sure you want to quit all applications and log out now?

If you do nothing, the system will automatically log out after a 2 minute wait.

After Logout - “nohup”

How to kill nohup processes

- LogoutHook
  - “killall -u $1”
    - Not very clean
  - killsumapps.pl
    - Kill all non-system user processes
  - And kill SUID

Q&A

Mac OS X Client Lab Security

Part 2

James Reynolds
Student Computing Labs
The University of Utah

Passwords

Safe password practices

- Use strong passwords
    - 8 characters minimum
    - Upper/lower case, numbers, symbols
    - No known word(s)
    - Phrase reduction
        - “I am me, sky by be!” 1@m,sbB!
    - Use a password generator

Passwords

Crack your own password

- John the Ripper
- See how long it takes

Change passwords often

- 6 months probably good

Passwords

Fix NetInfo world read permissions

- NetInfo Manager
- nicl, nidump, nifind, nigrep, niload, nireport, niutil
- /var/db/netinfo/local.nidb/
- /var/backups/local.nidump

Use unique local passwords

Passwords

Don’t use local users and passwords

- Password Server
- Kerberos
- LDAPv3 & SSL
- Enterprise Directory
    - Novell
    - Active Directory

SUID Root

What is SUID root?

- Set-UID
- Running a tool as the tool’s owner ID
- Joe runs non-SUID root tool (common)
    - Tool runs as Joe
- Joe runs SUID root tool (less common)
    - Tool runs as root

SUID Root

Secure SUID root tools

- Find them
    - “sudo find / -perm -4000 -user 0”
- Remove world execute permissions
- Do not add untrusted SUID root tools

SUID Root

“Useless” SUID root tools

- /bin/rcp
- /sbin/rdump
- /sbin/rrestore
- /usr/bin/rlogin
- /usr/bin/rsh
- More...

SUID Root

Useful SUID root tools

- /usr/sbin/netstat
- /sbin/ping
- /usr/sbin/traceroute
- /usr/bin/crontab
- More...

SUID Root

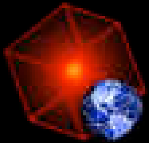
SUID root applications

- Disk Utility
- NetInfo Manager
- Classic: TruBlueEnvironment
- Finder.app: OwnerGroupTool
- System Prefs: readconfig, writeconfig
- Several printer utilities
- More...

SUID Root

3rd party applications

- Radmind Assistant
- Retrospect Client
- Virtual PC



Network Sniffing

Minimize threat of sniffing

- Use a smart switch or router
  - Lock ports to ethernet addresses
- Use secure applications
  - ssh, not telnet
  - sftp, not ftp
  - ssl email transfer

Services

Running server processes

- Only enable what is needed
- Configure access lists
- Enable firewall
    - Poke holes for legitimate ports

The Unknown

What if you are still compromised?

- Psychopath graduate cs students
- Forgetfulness
- Sneaky students
- Incompotent coworker

The Unknown

Configure ALL access lists, even if off

- Firewall
- sudoers
  - Replace “%admin” with <username>
- sshd
  - Add “AllowUser <username>”
  - Replace “Protocol 2,1” with “Protocol 2”

The Unknown

- TCP-Wrappers
  - /etc/hosts.allow
  - /etc/hosts.deny
  - inetd
  - xinetd
  - sshd
- httpd

The Unknown

Security scanners

- Nmap
  - Shows open ports
- Nessus
  - Scans open ports for vulnerabilities

The Unknown

Logs

- Use a central logger
  - syslogd
- Use a log checker
- Enable extra logging where possible
  - xinetd
  - Process accounting

Intrusion Detection

Types

- Honey Pot
  - Keep up to date!
- On router or switch
  - Privacy violation imminent
    - Contact Lawyers
- Snort
  - HenWen

Mac OS X Lab Security

More details available

- http://www.macos.utah.edu/macosx_security.html
- Scripts
- Links

Q&A