



# Mac OS X Security Overview

Dave Schroeder, UW DoIT ([das@doit.wisc.edu](mailto:das@doit.wisc.edu))

Matt Mueller, UW Medical School ([mmmuelle@wisc.edu](mailto:mmmuelle@wisc.edu))

[macosxlabs.org](http://macosxlabs.org)

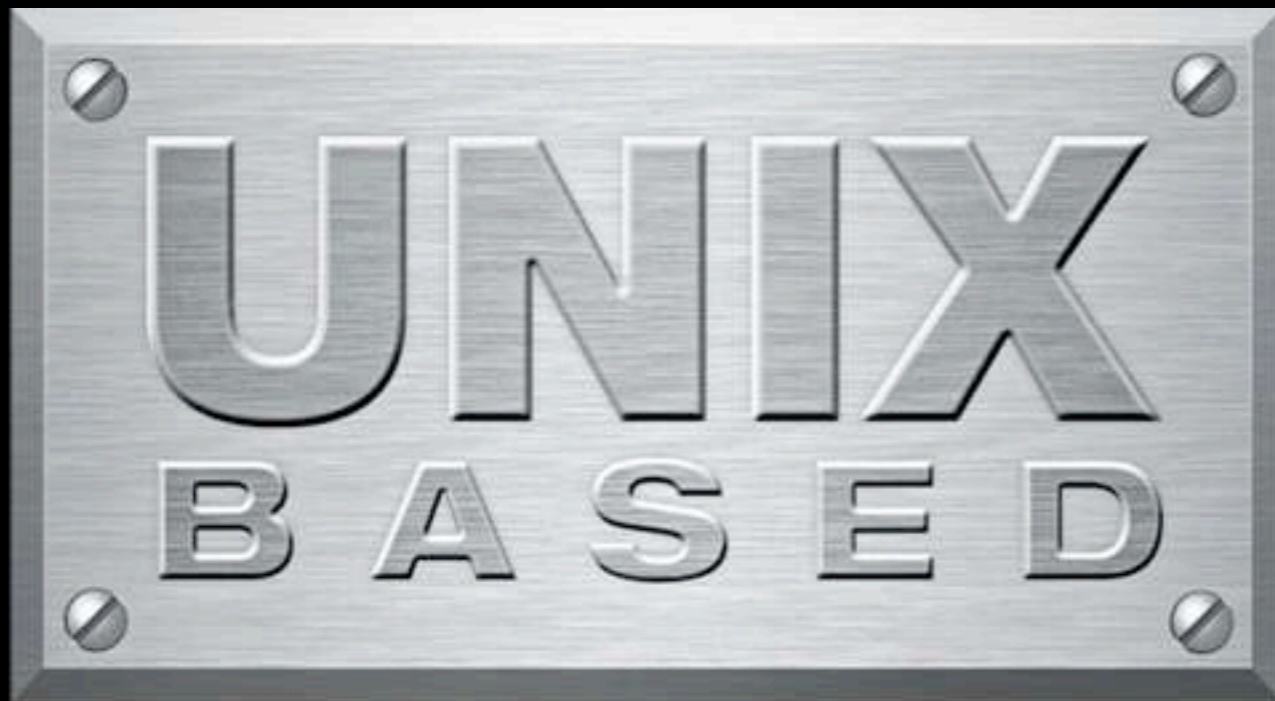
# Introduction

## Mac OS X Security Topics

- UNIX security features
- Data Encryption
- Extensibility
- Physical Security
- Security Updates
- Resources
- Technical Section

# UNIX Security

Open Standards and Open Source



Mac OS X is UNIX



Darwin is Open Source  
core of Mac OS X

Based on BSD 4.4 with  
enhancements

Panther (Mac OS X 10.3)  
has toolset parity with  
FreeBSD 5

# UNIX Security

## Open Standards and Open Source

- Compatible with other systems  
  - Can communicate with PCs and UNIX machines without compromising security
- Independent peer review and rapid evolution of source code
  - Security improvements contributed

# UNIX Security

## Popular and Open Standards

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

- OpenSSL



- Protects web and email communication

- Secure Shell

- OpenSSH



- Secure remote access from the command line; `ssh`, `scp`, `sftp`, etc.

# UNIX Security

## Secure Default Configuration

- Communication ports initially closed
- Default incoming remote access is `ssh`  
(not `telnet`)
- `root` user disabled
  - Use of `sudo` encouraged
- Ships with easy-to-use personal firewall  
(based on `ipfw`)

# Data Encryption

## Network Security Technologies

- Kerberos
- Supports X.509 digital certificates
- Wired Equivalent Privacy (WEP) encrypts wireless traffic



# Data Encryption

## Network Security Technologies

- Supports Virtual Private Network (VPN) using Point-to-Point Tunneling Protocol (PPTP)
  - Secure access to educational and corporate networks
- IPv6 and IPSec are implemented

# Data Encryption

## Network Security Technologies

- Apple Password Server
  - Simple Authentication and Security Layer (SASL) based
  - Password never passed over network, like Kerberos
  - Works with Workgroup Manager to enforce secure passwords
  - Support in Mac OS X Server and Mac OS X

# Data Encryption

## Local Security Technologies

- Supports USB Smart Card devices
  - Digital certificates can be carried on cards and used on other machines



- Supports biometric identification (Sony fingerprint identification suite, etc.)



- Disk Copy can create disk images and volumes encrypted with Advanced Encryption Standard (AES) 128-bit



# Data Encryption

## Local Security Technologies



- Keychain provides single secure password and permission store
  - Stores certificates, credentials, passwords (email, web, form, file server, etc.)
  - Multiple user support to ensure privacy
  - Data stored in Triple Digital Encryption Standard (3DES)

# Extensible

## Open Standards and Open Source

- Common Data Security Architecture (CDSA) allows creation of flexible security services
- Integrated Pluggable Authentication Module (PAM) support
  - UNIX applications gain access to built-in authentication mechanisms

# System Security

## Protecting Deployed Machines

- Use Open Firmware passwords
  - Disables startup manager and hot keys for single user mode, CD booting, etc.
  - Use Apple's Open Firmware Password tool to enable
- Use hardware locks
- Disable Auto Login
- Xserve and Xserve RAID monitored for intrusion



# Security Updates

Stay aware of vulnerabilities!



- Distributed via Software Update mechanism
  - Accessible via System Preferences or command line
  - Updates digitally signed to verify source
- Distributed standalone with documentation
- Apple responds quickly to vulnerabilities
  - Report to [product-security@apple.com](mailto:product-security@apple.com)

# Security Updates

Stay aware of vulnerabilities!

- [security-announce at lists.apple.com](mailto:security-announce@lists.apple.com)
- [apple.com/support/security/](https://apple.com/support/security/)
- [apple.com/macosx/technologies/security.html](https://apple.com/macosx/technologies/security.html)
- Industry security resources such as CERT, SecurityFocus, etc.

# Security Updates

Stay secure!

- Don't enable unneeded services
- Use tools to ensure machines are up to date

- Apple Remote Desktop



- `system_profiler`



- Use utilities to monitor/clean up machines

- `radmind`



- `rsyncx`

# Resources

Apple Security:

[apple.com/support/security/](http://apple.com/support/security/)

[security-announce at lists.apple.com](mailto:security-announce@lists.apple.com)

[apple.com/download/](http://apple.com/download/)

[developer.apple.com/internet/macosex/securityintro.html](http://developer.apple.com/internet/macosex/securityintro.html)

Mac OS X Higher Education Deployment Initiative:

[macosxlabs.org](http://macosxlabs.org)

DoIT Apple Support: [apple.doit.wisc.edu](http://apple.doit.wisc.edu)

University of Utah Mac OS X security:

[www.macos.utah.edu/macosex\\_security.html](http://www.macos.utah.edu/macosex_security.html)

Princeton Mac OS X security:

<http://www.princeton.edu/~psg/unix/osx/osxsecurity.html>

# Books



Mac OS X: The Missing Manual

[www.oreilly.com/catalog/macosexmm2/](http://www.oreilly.com/catalog/macosexmm2/)

\$29.95



Mac OS X in a Nutshell

[www.oreilly.com/catalog/macosexian/](http://www.oreilly.com/catalog/macosexian/)

\$34.95



Mac OS X for UNIX Geeks

[www.oreilly.com/catalog/mosxgeeks/](http://www.oreilly.com/catalog/mosxgeeks/)

\$24.95

Q & A

# Technical Section

A little background...

# Startup

- No `/etc/rc*.d/` or `/etc/init.d/` for starting system startup files
- Replaced by `/System/Library/StartupItems/` (system provided) and `/Library/StartupItems/` (user installed)
- Login Items started in System Preferences
- SystemStarter - start/stop system services

# Directory Services

- By default, no Unix flat files
- NetInfo stores info about users and resources (/etc/passwd /etc/host)
- NetInfo db located in /var/db/netinfo
- NetInfo Manager - GUI utility for editing the db (but be CAREFUL!)

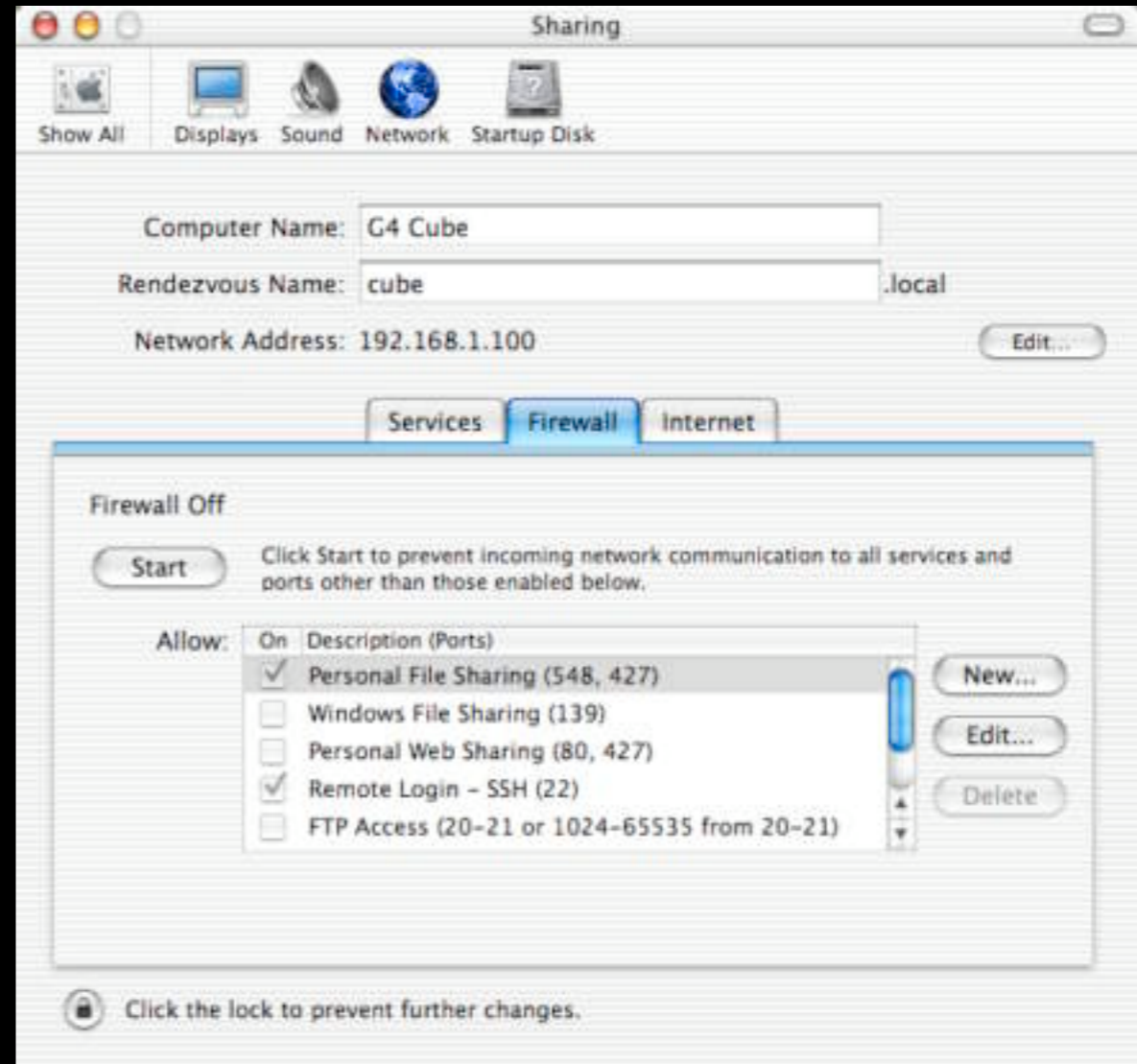
# Logs

- Most in `/var/log`
- Some in `/Library/Logs`
- `/Library/Receipts`
- `wtmp` in `/var/log` and `utmp` in `/var/run`
- Scripts in `/etc` (daily, weekly, monthly)  
control rotation of logs

# Prevention and Detection

# Built-In Firewall

- Firewall is BSD based
- Configuration thru the Sharing tab in System Preferences (just TCP ports)
- Command line tool, ipfw, is more versatile
- BrickHouse, sunShield



# IDS & Logs

- No built-in IDS, install a third party tool such as Snort
- Change default logging for web or ftp server
- By default, /etc/daily removes web logs after seven days
- LogSentry for log monitoring  
(logsentry-1.1.1.tar.gz)

# Tools

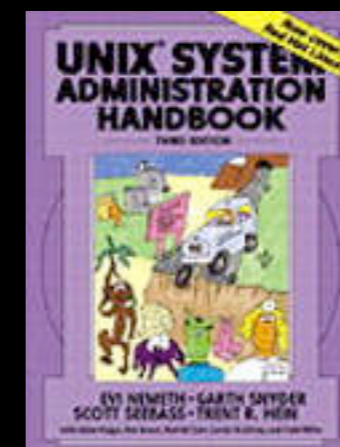
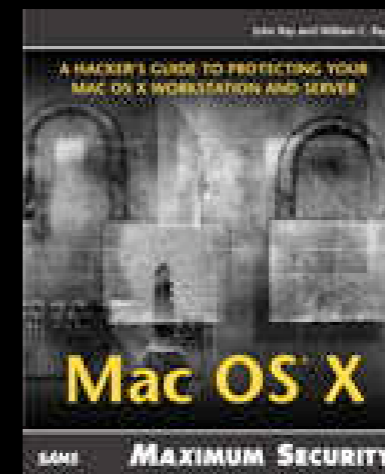
- nmap
- TripWire (Prebinding)
- ctool - smart checksumming  
<http://www.macsecurity.org/tools/ctool/>
- chkrootkit - check binaries for rootkits  
[www.chkrootkit.org](http://www.chkrootkit.org)  
<http://www.oreillynet.com/pub/au/776>

# More Links

- <http://homepage.mac.com/macbuddy/SecurityGuide.html>
- <http://www.knowngoods.com/>
- <http://www.osxfaq.com/Tutorials/lockdown/index.ws>
- <http://www.osxfaq.com/Editorial/security/index.ws> (index2.ws & index3.ws)
- <http://developer.apple.com/internet/macosx/securityintro.html>
- <http://www.princeton.edu/~psg/unix/osx/osxsecurity.html>

# Books

- Mac OS X *for* Unix Geeks
- Maximum Mac OS X Security
- Unix System Administration Handbook



# Acknowledgments

- Mac OS X Higher Education Deployment Initiative
  - [macosxlabs.org](http://macosxlabs.org)
- Apple University Executive Forum
- Joe Jackson, Carnegie Mellon University
- Jeff Greene, University of Colorado
- James Reynolds, University of Utah

This seminar is  
available from:

[apple.doit.wisc.edu/  
news/seminars/](http://apple.doit.wisc.edu/news/seminars/)

Q & A

