Mac OS X Security and System Hardening

Dreux Ste. Marie
Systems Engineer

“Qui non est hodie cras
minus aptus erit.”

“He who is not prepared today
will be less so tomorrow.”

Ovid

Mac OS X Security and System Hardening

Agenda

- Security Features of Mac OS X
- System Hardening
  - Top 10 Steps to Mitigate Risk
- Resources

Part 1:

Security Features of Mac OS X

Mac OS X Security

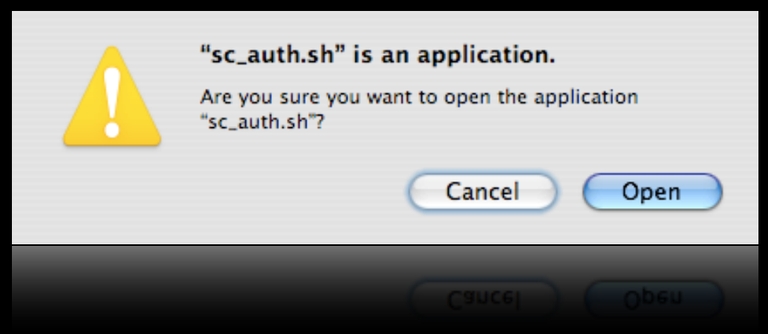
UNIX Foundation

- Official UNIX 03 Registered Product
- Full POSIX API Compliance
- Optimized for Multicore
- Secure
- Scalable
- Open Standards
- High Performance
- Rock-Solid Stability
- Advanced Networking

Mac OS X Security

Conservative Defaults And Security Policies

- Services Off and Ports Closed
- Root Account Disabled
- New Users "Standard," Not "Admin"
- Authentication to Install Applications and Change Settings
- Safe Mail Attachment Handling



Mac OS X Security

Layers of Protection

- Physical Security
  - Kensington Security Lock Slot Available
    - MacBook, MacBook Pro, Mac mini, iMac
    - Not Available on MacBook Air
  - Built-in Enclosure Lock
    - Mac Pro
    - Xserve

Mac OS X Security

Layers of Protection

- Strong Authentication
  - Unified Authentication for:
    - Login, Wake, and Screen Saver
    - Changing System Settings
    - Single Sign-on
  - Authentication for Application Installation
  - Cached Credentials for Offline Authentication

Mac OS X Security

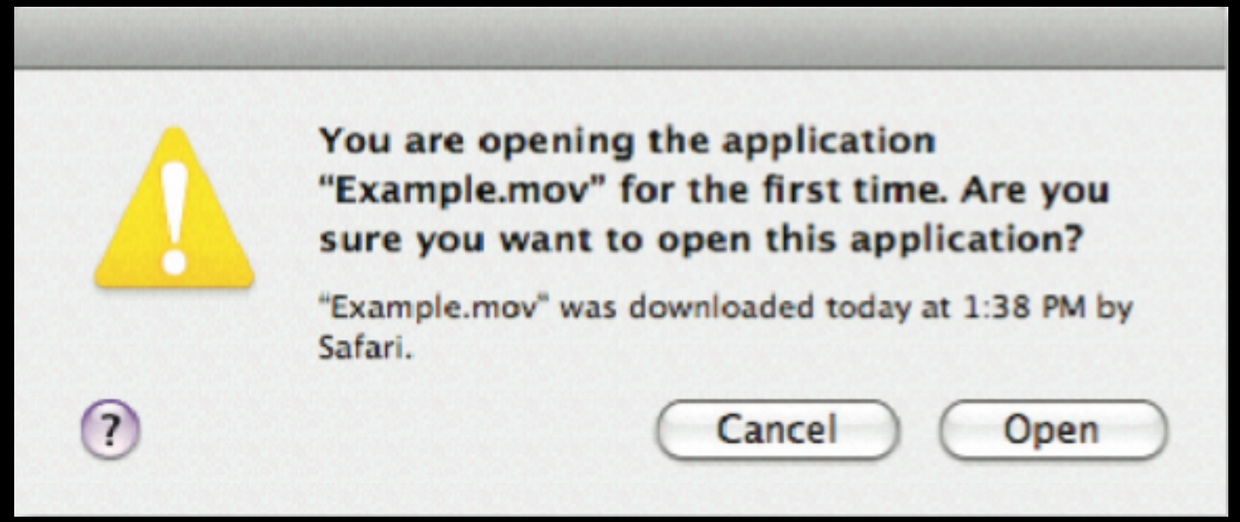
Layers of Protection

- Strong Authentication
  - Smart Cards
    - Lock System on Smart Card Removal
    - Unlock Keychain
    - Unlock FileVault
  - Biometrics
    - Fingerprint Readers

Mac OS X Security

Layers of Protection

- Mandatory Access Controls
- Protection Against Trojan Horse Applications



Mac OS X Security

Secure Network Communications

Mac OS X Security

Runtime Protection

- Execute Disable (XD)
  - Feature of Intel Processors
  - Processor Refuses to Execute Instructions that Might be Buffer Overflows
- Library Randomization
  - Prevents “return to libc” Attacks
  - Libraries are Loaded into Random Addresses at System Install/Update
- Sandboxing
  - Ensures Apps Only Do What They’re Intended to Do
  - Restricts Which Files They Access
  - For Example, Spotlight, Quick Look, mDNSResponder, Kerberos KDC

Mac OS X Security

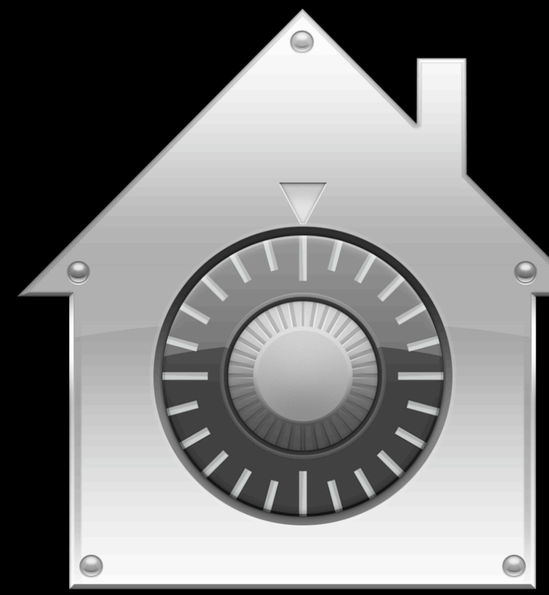
Application Signing

- All Leopard Apps Are Signed
- Used by Parental Controls, Managed Preferences, Keychain, Firewall
- Ensures App is Non-Modified

Mac OS X Security

Protecting Private Data

- FileVault
- Encrypted Disk Images (EDI)
- Secure Empty Trash
- Encrypted Virtual Memory
- Private Browsing
- Guest Account



Cyberdiversity

"By spreading critical business functions across multiple desktop platforms or by maintaining key operating groups on separate platforms, you can enhance your ability to keep at least some of your key personnel and processes functioning and communicating during an attack."

Gartner Group

Part 2:

System Hardening

System Hardening

Definition

Reduce or Eliminate as Many Security Risks as Possible, Given the Environment in Which the System is Functioning.

Steps

- Start Protected
- Maintain Good Protection
- Validate System Integrity
- Notification

10 Steps to Mitigate Risk

Start Protected

Start with a Clean Slate

Work From a Known-Good State

1

- Clean Install of Mac OS X
  - Use Original Installation Media, if Possible
- Re-Image Mac With a Qualified Institutional Image
- Do Not Assume a Mac Is in an Acceptable State

- Apple Tools/services to Use
  - Mac OS X Install DVD
  - Disk Utility
  - asr
  - NetInstall

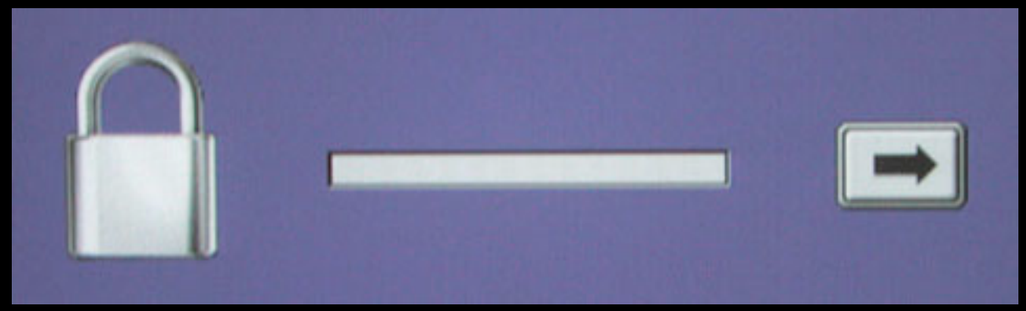
Secure the Host

Lockdown System Startup

2

- Firmware Lockdown to OS Boot Instance
  - Firmware-Based ‘Password’ – Not an Account
  - Locks Boot Instance to the Partition’s GUID
  - FireWire Drives Use a Bridge Chip (Chip is GUID)

- Apple Tools/services to Use
  - Open Firmware Password Utility (PPC OF)
  - Firmware Password Utility (Intel EFI)



Secure the Host

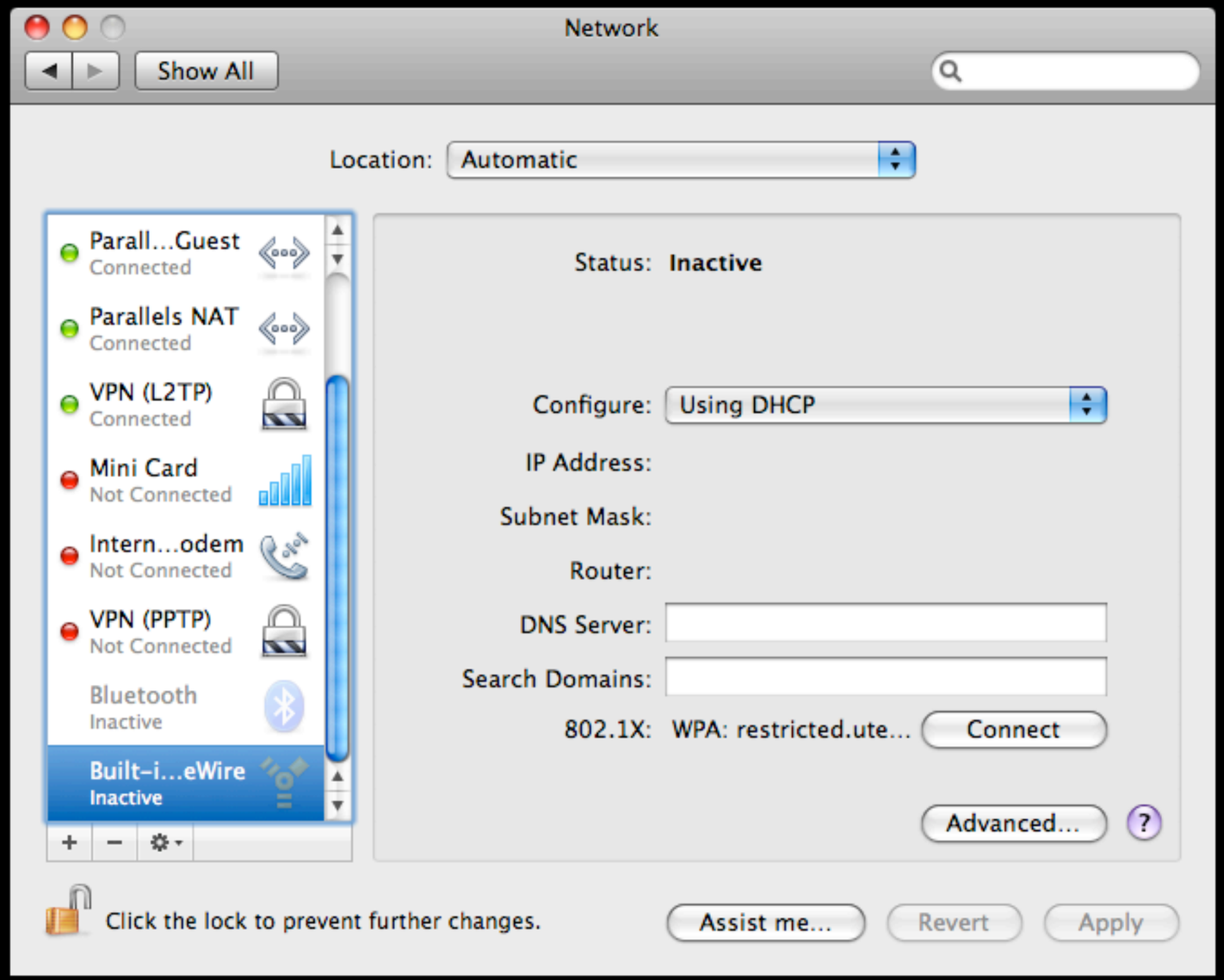
Disable Unused Network Interfaces

2

- Disable Hardware Ports Not in Use
- Disable RF (Wi-Fi, Bluetooth) in Non-Secure Areas
- Disable "Discoverable" Beyond Setup Time

- Apple Tools/services to Use
  - System Preferences (Local Management)
  - WorkGroup Manager (Centralized Management)
  - Terminal (CLI Modification of Services)

Demo


Network
Show All
Location: Automatic
Parall…Guest
Connected
Parallels NAT
Connected
VPN (L2TP)
Connected
Mini Card
Not Connected
Intern…odem
Not Connected
VPN (PPTP)
Not Connected
Bluetooth
Inactive
Built-i…eWire
Inactive
Status: Inactive
Configure: Using DHCP
IP Address:
Subnet Mask:
Router:
DNS Server:
Search Domains:
802.1X: WPA: restricted.ute…
Connect
Advanced…
Click the lock to prevent further changes.
Assist me…
Revert
Apply

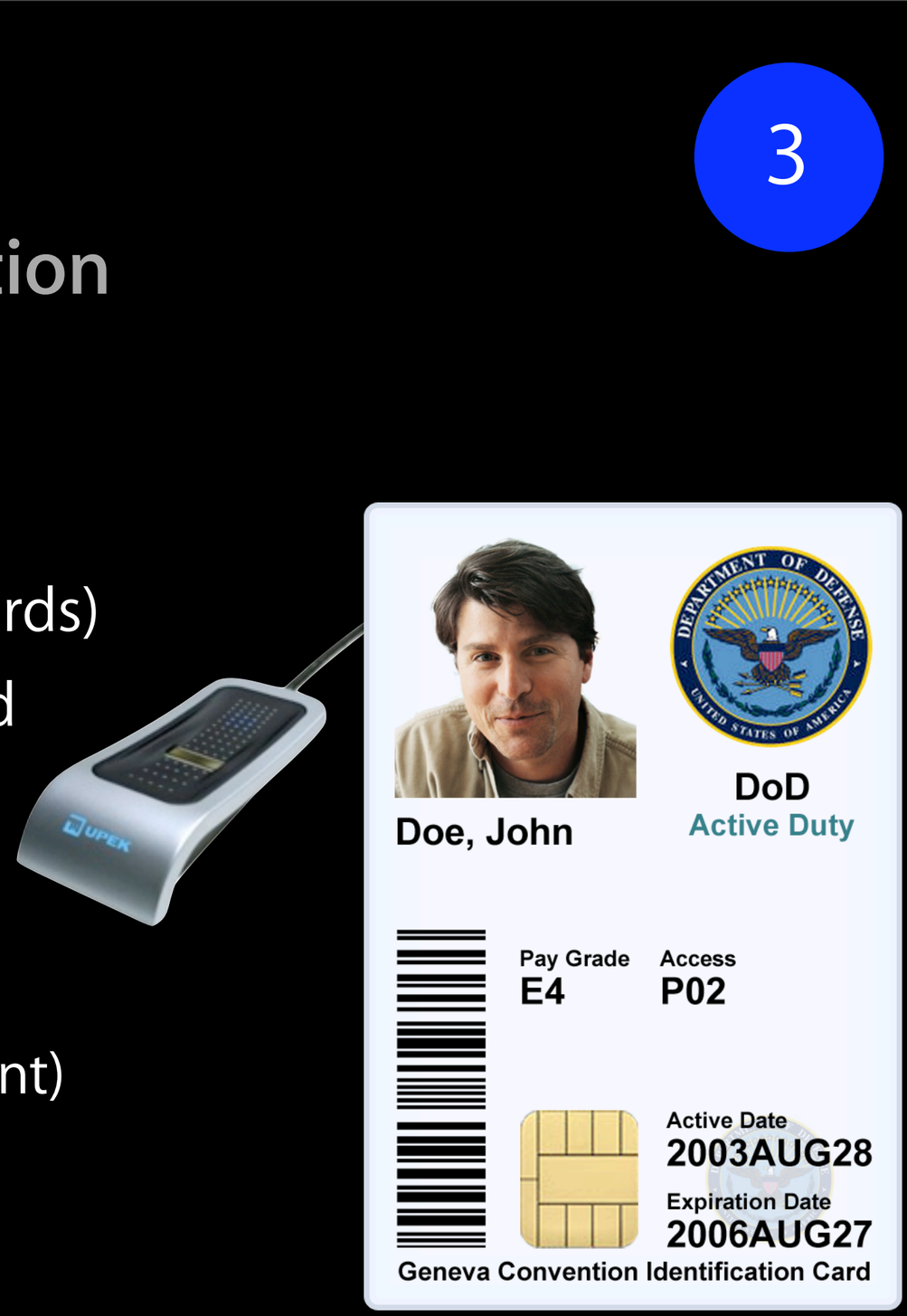
User Authentication

Use Secure and Reliable Authentication

3

- DO NOT Operate Under an Admin Account
- DO NOT Enable the ROOT Account
- Use Two-Factor Authentication (i.e., Smart Cards)
- Modify Authorization Rights/Rules as Needed

- Apple Tools/services to Use
  - System Preferences (Local Management)
  - WorkGroup Manager (Centralized Management)
  - Terminal (CLI Modification of Services)



Maintain Good Protection

Securing Data and Using Encryption

Protection of Data at Rest (DAR) AES-128/AES-256

4

- FileVault for Users' Home Directory
- Portable Encrypted Storage Containers (EDI)
- Enable Secure Virtual Memory
- Backup EDIs via Time Machine (Leopard)

- Apple Tools/services to Use
  - System Preferences (Local Management)
  - WorkGroup Manager (Centralized Management)
  - Disk Utility (Encrypted Disk Image Creation/Management)
  - Terminal ('hdiutil' Command)

Encrypted Storage—Disk Images

Encrypted Data on Any Accessible Storage Device

4

- Encrypted Disk Images(EDIs) Are Accessible as Logical Volumes and Physically Stored as Encrypted Files.
- Disk Images Can be Stored on Any Accessible Storage Media.
  - External Drives (USB/FireWire)
  - Optical Disks (CD/DVD)
  - Network Volumes
  - Flash Media
- Leopard Introduces AES-256

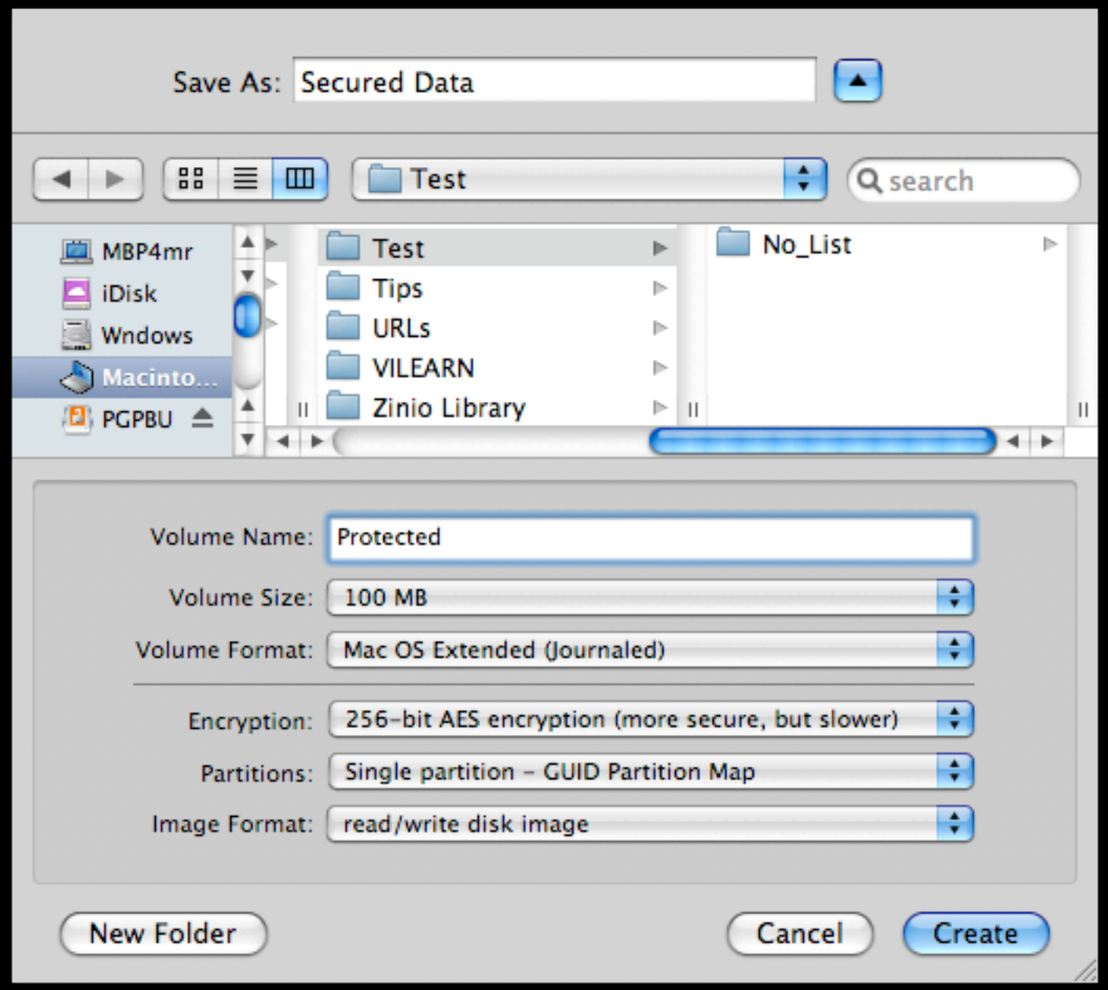
Encrypted Storage—Disk Images

4

Encrypted Data on Any Accessible Storage Device

- Easily Distribute Encrypted Images and Control Access
- Multiplatform and Multidisk Format Support
  - Parallels With Other OSes Locally or Remotely on a Server
  - HFS+, UFS, FAT32

Demo


Save As: Secured Data
Test
search
MBP4mr
iDisk
Wndows
Macinto...
PGPBU
Test
Tips
URLs
VILEARN
Zinio Library
No_List
Volume Name: Protected
Volume Size: 100 MB
Volume Format: Mac OS Extended (Journaled)
Encryption: 256-bit AES encryption (more secure, but slower)
Partitions: Single partition - GUID Partition Map
Image Format: read/write disk image
New Folder
Cancel
Create

Securing Active Services

Know What Services You Are Running and Why

5

- Disable or Even Remove All Unused Services
- Use security Enhanced Versions of UNIX Tools
- Leverage Service ACLs—Fine-Grained Control

Secure	Insecure
ssh	telnet
scp	cp
srm	rm

- Apple Tools/services to Use
  - System Preferences (Local Management)
  - Server Admin (Server Management)
  - Terminal (CLI Commands)

Enable Firewall if Active Services

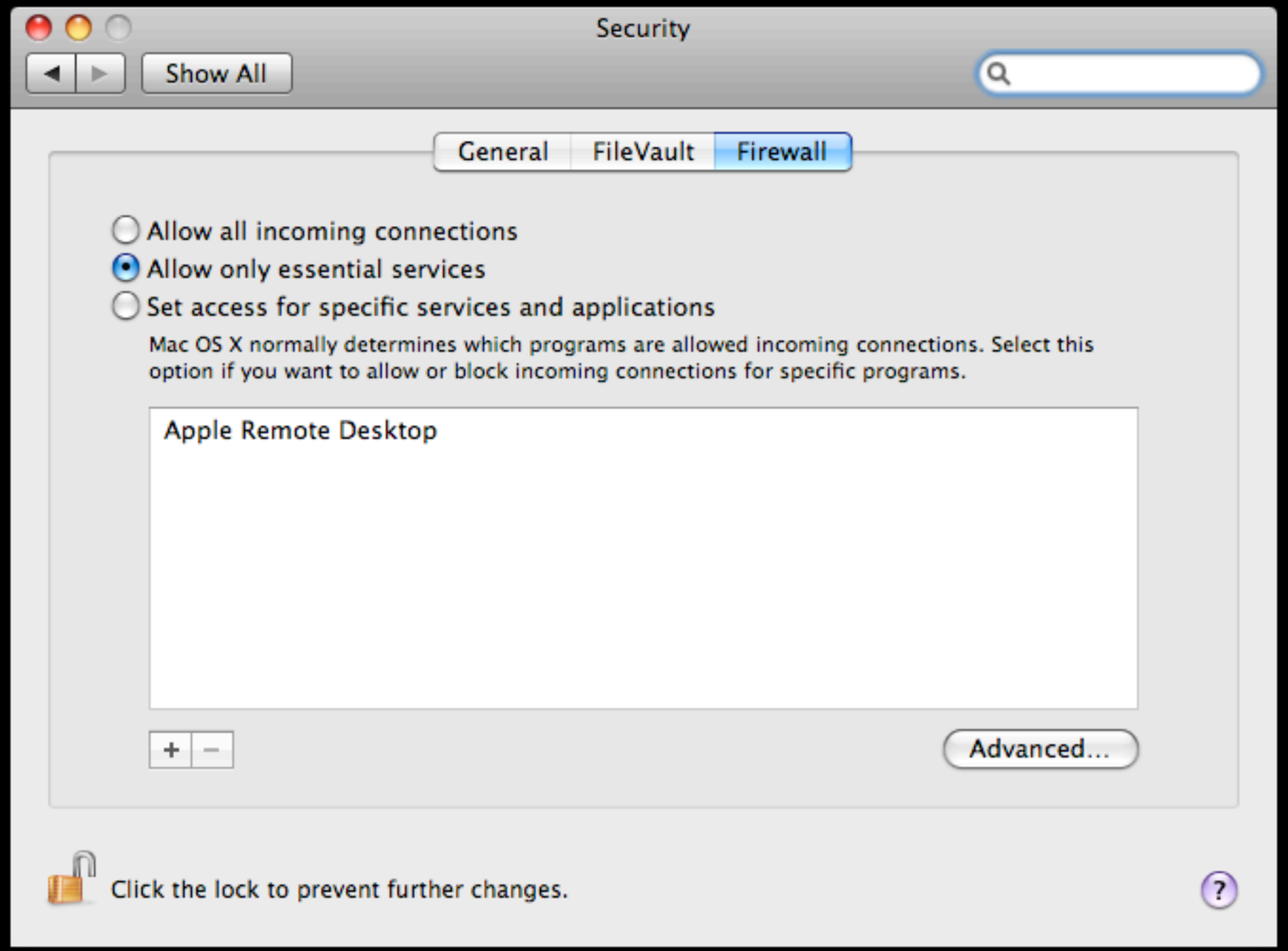
Know What Services You Are Running and Why

6

- Barrier to Prevent Unauthorized Access
  - Enable if You Are Running ANY Services
  - Enable "Stealth Mode" (Tiger)
  - Limit Incoming Connections (Leopard)

- Apple Tools/services to Use
  - System Preferences (Local Management)
  - Server Admin (Server Management)
  - Terminal (CLI Commands)

Demo


Security
Show All
General
FileVault
Firewall
Allow all incoming connections
Allow only essential services
Set access for specific services and applications
Mac OS X normally determines which programs are allowed incoming connections. Select this option if you want to allow or block incoming connections for specific programs.
Apple Remote Desktop
+
−
Advanced...
Click the lock to prevent further changes.
?

Maintain System/Application Updates

7

- Maintain a Fortified Posture
  - Heed Security Notifications From Apple
  - Apply Security Patches
  - Maintain Vigilance With Third-Party Applications
  - Track Changes to Self-Installed Open Source Projects

- Apple Tools/services to Use
  - System Preferences (Software Update)
  - Server Admin (Software Update Server)
  - Apple Remote Desktop (Push Updates)
  - Terminal (CLI Commands)

Validate System Integrity

Install Virus Protection

8

- Pick a Secutiry Reputable Vendor
  - -Symantec
  - -Intego
  - -MacAffee
  - -Sophos

McAfee®

SOPHOS

- Practice Responsible Behaviors On-Line
  - Avoid Pirate Sites
  - Avoid Porn Sites
  - Avoid Downloads from Untrusted Sites

Audit Security-related Events

9

- Auditing Goes Beyond Logging
  - Continuously Audit the Relevant Events
    - BSM (Basic Security Module) is Built into Mac OS X
    - Common Criteria Admin Guide/Security Config Guide
    - CC_Tools Provides
      - Audit, Auditd, Auditreduce, Praudit (CLI Commands)
      - Audit Log Viewer (GUI Utility for Audit Log Viewing)

- Apple Tools/services to Use
  - Audit Log Viewer (GUI Utility for Audit Log Viewing)
  - Terminal (CLI Commands)

Notification

Legal Notification of Usage

10

- Login Banners With Legal Notifications
  - Modify Login Window .plist With Banner Text
  - Utilize AuthPlugins and Create Your Own
  - LoginWindow Manager From Bombich.com

- Apple Tools/services to Use
  - Xcode (AuthPlugin)
  - Terminal (CLI Commands)

Part 3:

Resources

Resources

Apple

- To Report Security Issues to Apple, Contact: product-security@apple.com
- Apple Product Security
  - http://www.apple.com/support/security/
- Apple Security Updates
  - http://docs.info.apple.com/article.html?artnum=61798
- Security Features in Leopard
  - http://www.apple.com/macosx/features/300.html#security
- Common Criteria
  - http://www.apple.com/support/security/commoncriteria/

Resources

Apple

- Security-Announce Mailing List
  - http://lists.apple.com/mailman/listinfo/security-announce
  - feed://rss.lists.apple.com/security-announce.rss
- Developer Info
  - http://developer.apple.com/security/
  - http://developer.apple.com/internet/security/securityintro.html
  - http://developer.apple.com/opensource/security/

Q&A