Why Is My Mac So Insecure?

The Mac OS X Security Myth Exposed

Marko Jung & James Partridge
NSMS

"Mac OS X is like living in a farmhouse in the country with no locks, and Windows is living in a house with bars on the windows in the bad part of town."

"Mac OS X is like living in a farmhouse in the country with no locks, and Windows is living in a house with bars on the windows in the bad part of town."

Source: Charlie Miller, Independent Security Evaluators

Windows vs OS X

2007 - all CVEs without third party software

Sources: ZDnet, National Vulnerability Database

Windows vs OS X

2007 - all CVEs without third party software

Sources: ZDnet, National Vulnerability Database

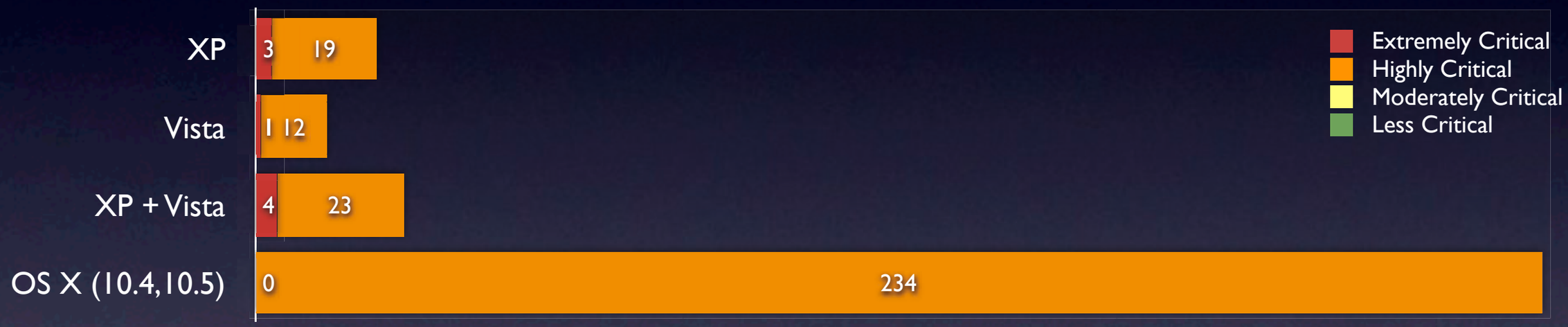
Windows vs OS X

2007 - all CVEs without third party software

Sources: ZDnet, National Vulnerability Database

Windows vs OS X

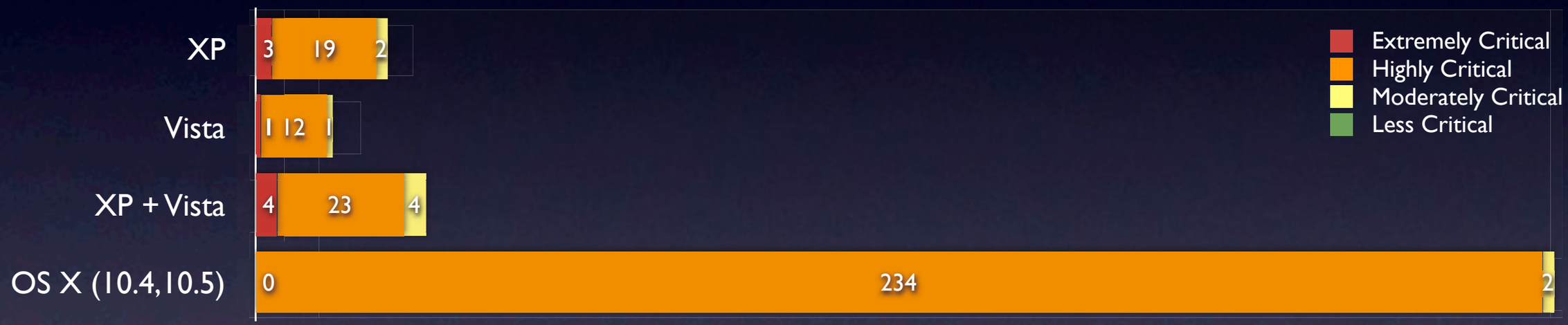
2007 - all CVEs without third party software



Sources: ZDnet, National Vulnerability Database

Windows vs OS X

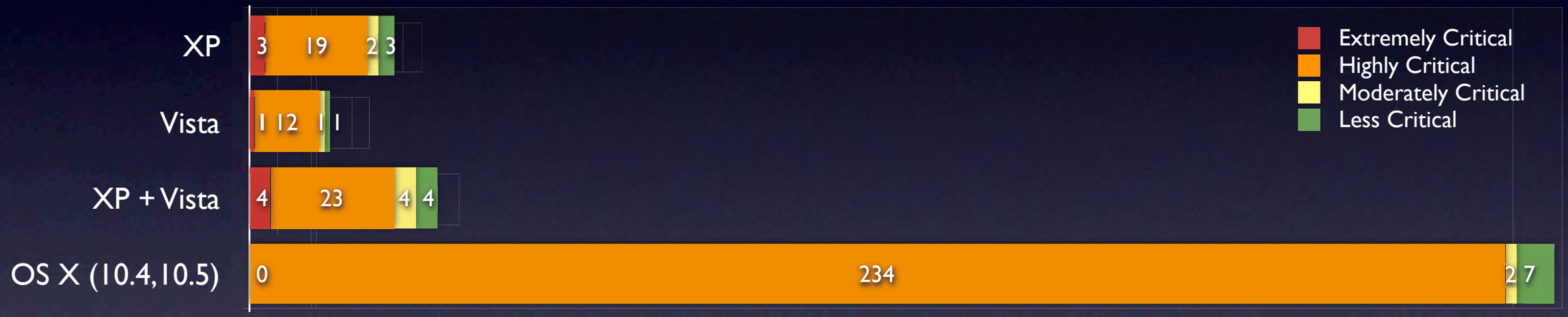
2007 - all CVEs without third party software



Sources: ZDnet, National Vulnerability Database

Windows vs OS X

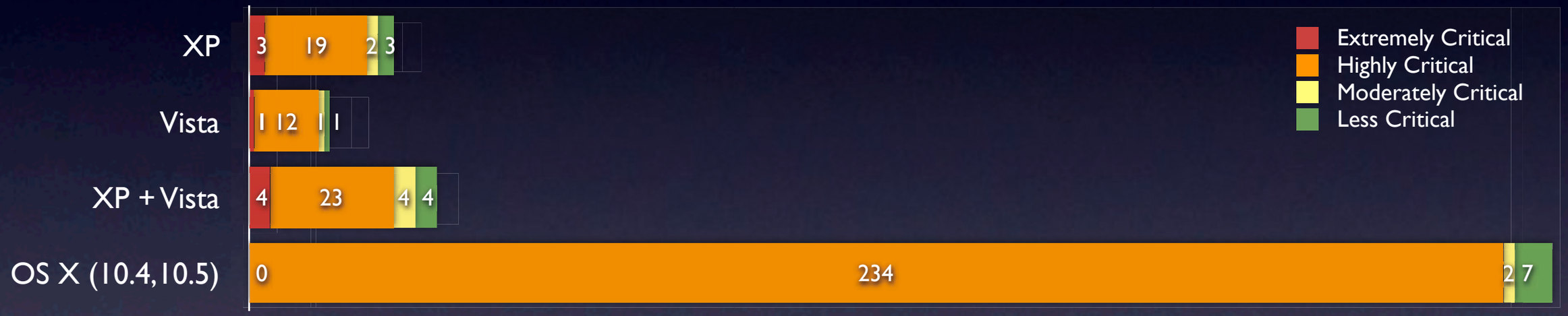
2007 - all CVEs without third party software



Sources: ZDnet, National Vulnerability Database

Windows vs OS X

2007 - all CVEs without third party software

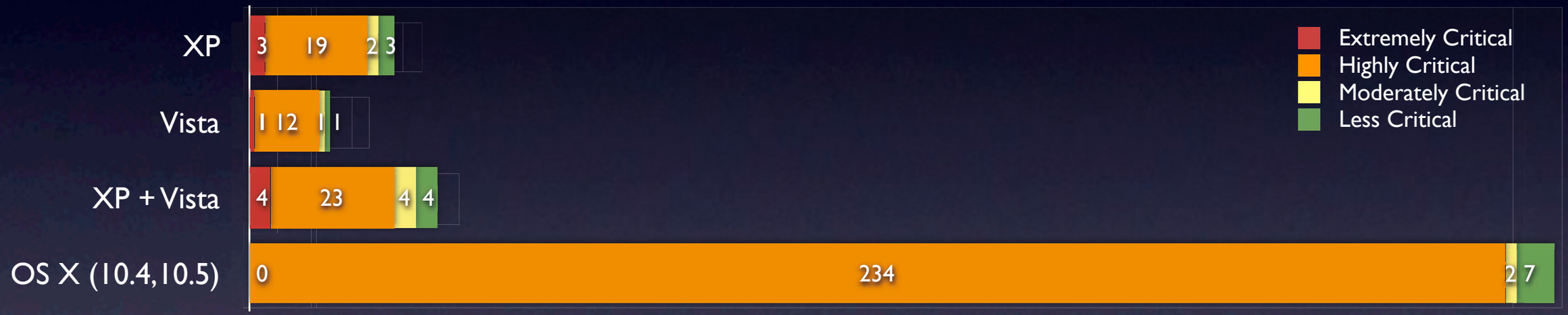


09/2009 - 07/2010 - all CVEs without third party software

Sources: ZDnet, National Vulnerability Database

Windows vs OS X

2007 - all CVEs without third party software

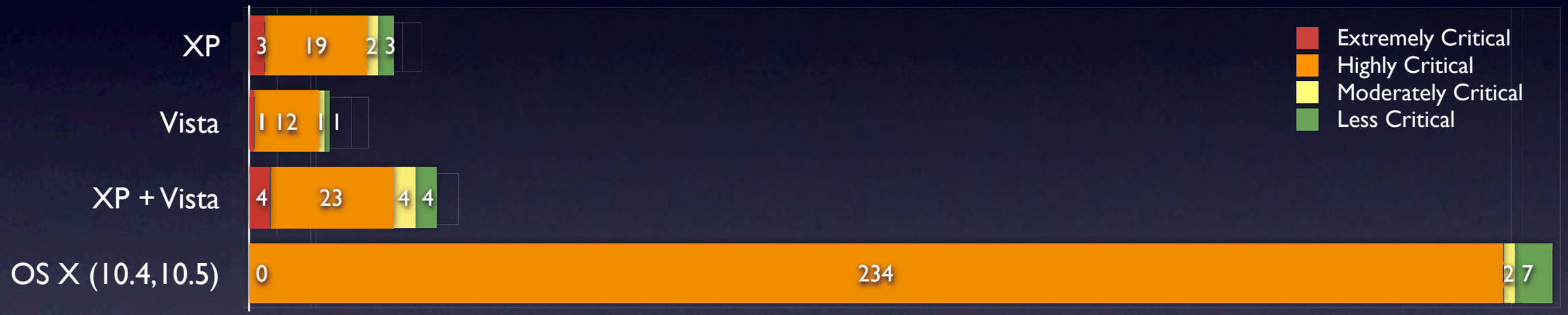


09/2009 - 07/2010 - all CVEs without third party software

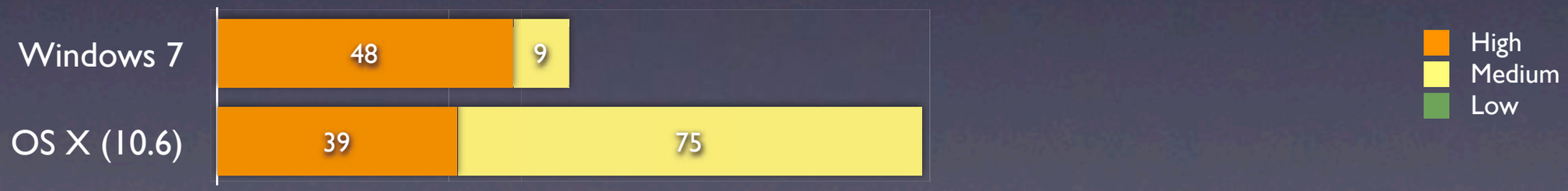
Sources: ZDnet, National Vulnerability Database

Windows vs OS X

2007 - all CVEs without third party software



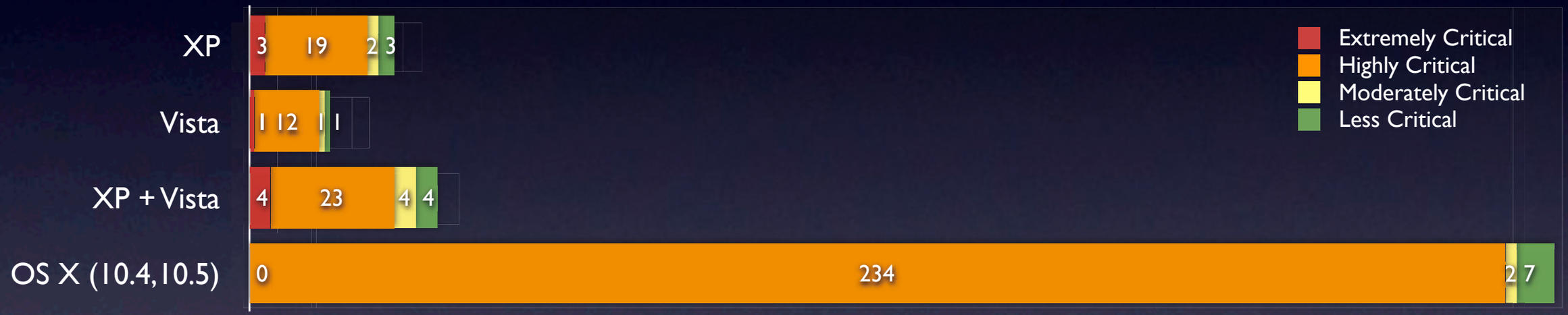
09/2009 - 07/2010 - all CVEs without third party software



Sources: ZDnet, National Vulnerability Database

Windows vs OS X

2007 - all CVEs without third party software



09/2009 - 07/2010 - all CVEs without third party software

Sources: ZDnet, National Vulnerability Database

Impact levels

- Denial of service (locally or remote)
- Disclosure of information:
  - authentication
  - system
  - user
- Modification of information
  - authentication
  - system
  - user
- Execution of arbitrary code (local or remote)
- Host/resource access via network
  - User access (local or remote)
  - Root access (local or remote)

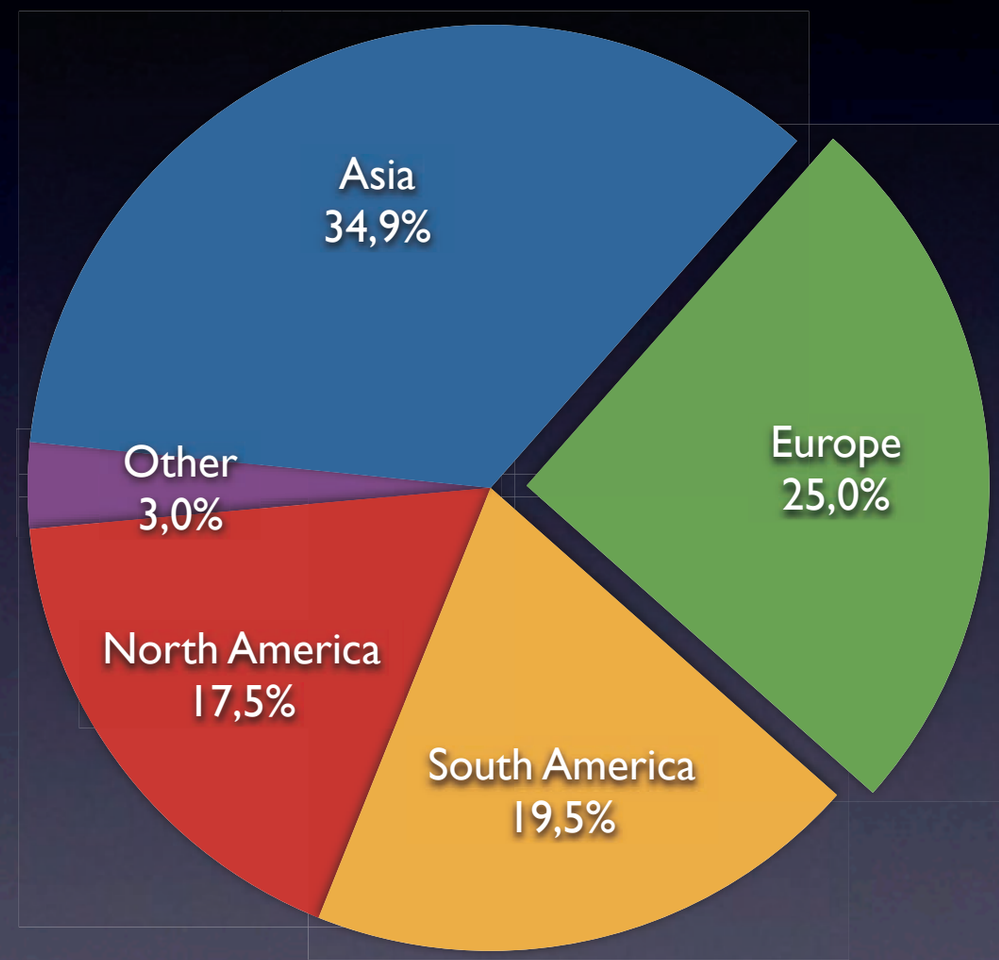
E-Mail

Email threats

- Hostile content in message or attachment
- Deliver malicious code or visit a malicious website
- Spam is often an entry point for scams, fraud, dirty tricks or malicious action.

Email threats

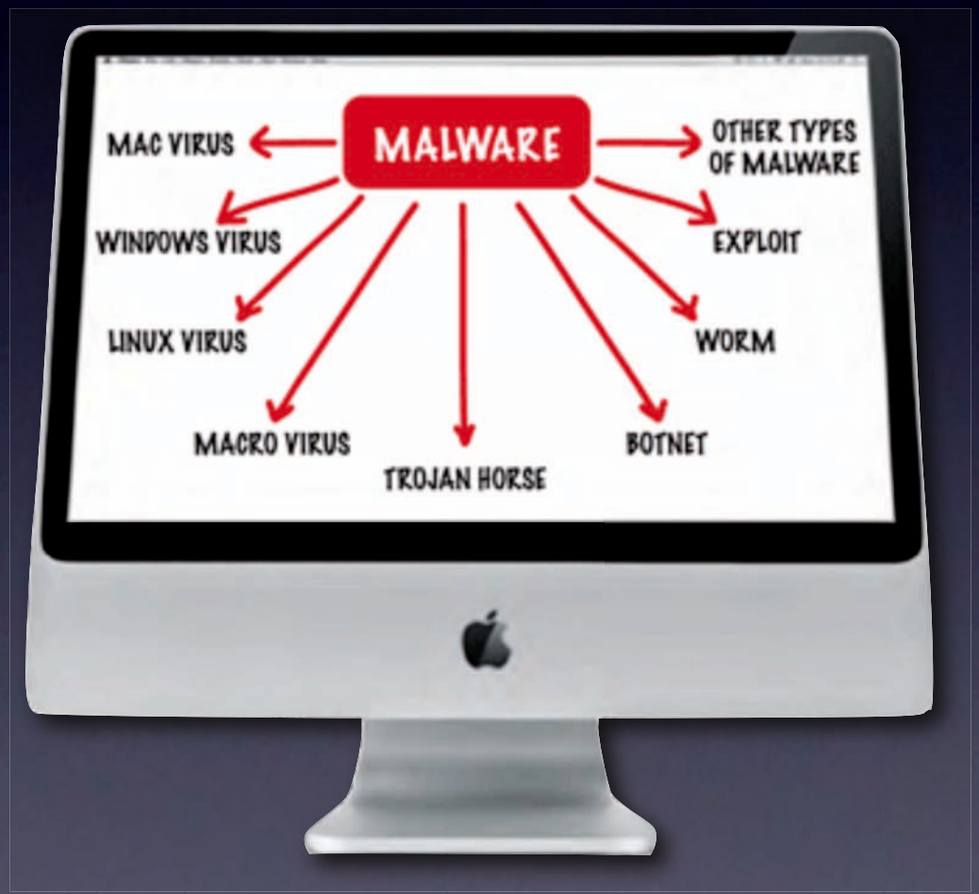
- Hostile content in message or attachment
- Deliver malicious code or visit a malicious website
- Spam is often an entry point for scams, fraud, dirty tricks or malicious action.



Spam by continent

Source: Sophos Security Threat Report 2010

Malware



- Viruses (including Macros)
- Trojan Horses
- Worms
- Botnets
- Keyloggers
- Spyware, Adware
- Exploits

Illustration: Intego

Foistware & Fake AV

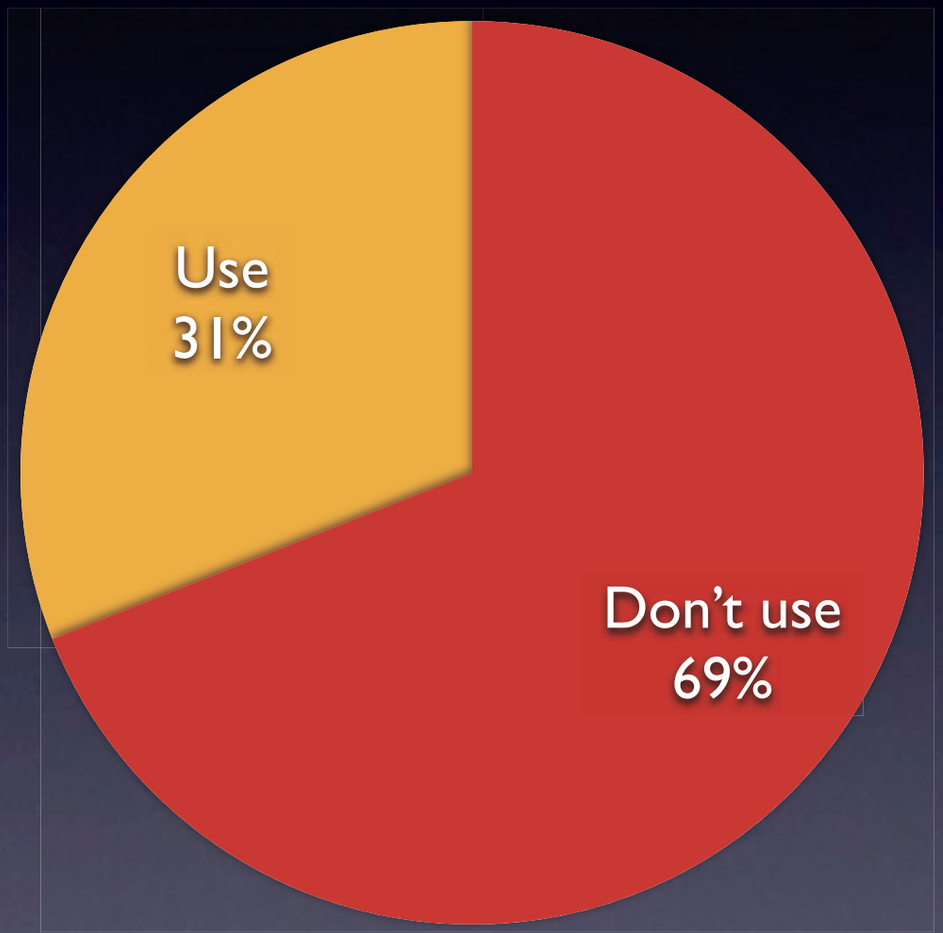
Foistware (sneakware) is growing on the Mac platform, eg. iWorkServices

Fake anti-virus software scams are no longer limited to Windows, but they were harmless scareware.

Virus Scanners

Sophos survey mid-2009 showed that 69% of Mac users don't use anti-virus software.

Sophos currently lists analyses of 31 Mac malwares, almost all Trojans (some variants of each other)



Do you use anti-virus to protect your Mac?

Source: Sophos Security Threat Report 2010

Safer choice

For University owned Macs always use Oxford's non-expiring Sophos installation

Educate your users to download Sophos for their personal machines from register.oucs.ox.ac.uk

Web

Web threats

- Attacks use power of modern browsers:
  - dynamic content (script) languages
  - plug-ins
- Malicious ads, iFrames and popup windows
- Downloads

Web threats

- Attacks use power of modern browsers:
  - dynamic content
  - (script) languages
  - plug-ins
- Malicious ads, iFrames and popup windows
- Downloads

Quarantine

Quarantine

Quarantine

- Quarantined apps are checked for malware listed in: **`/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist`**

Quarantine

- Quarantined apps are checked for malware listed in: **`/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist`**

- Quarantine is only supported by some apps, e.g. browsers, Mail (& Thunderbird), iChat, Entourage. Won't work in other cases, e.g. file from BitTorrent, FTP. Full list of (11) supported apps in **`Exceptions.plist.`**

Quarantine

- Quarantined apps are checked for malware listed in: **`/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist`**

- Quarantine is only supported by some apps, e.g. browsers, Mail (& Thunderbird), iChat, Entourage. Won't work in other cases, e.g. file from BitTorrent, FTP. Full list of (11) supported apps in **`Exceptions.plist.`**

- Finder NOT protected (so copying Trojans from USB sticks isn't detected!).

Quarantine

- Quarantined apps are checked for malware listed in: **`/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist`**

- Quarantine is only supported by some apps, e.g. browsers, Mail (& Thunderbird), iChat, Entourage. Won't work in other cases, e.g. file from BitTorrent, FTP. Full list of (11) supported apps in **`Exceptions.plist.`**

- Finder NOT protected (so copying Trojans from USB sticks isn't detected!).

- Trojans hidden within .mpkg files not detected.

Quarantine

- Quarantined apps are checked for malware listed in: **`/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist`**
- Quarantine is only supported by some apps, e.g. browsers, Mail (& Thunderbird), iChat, Entourage. Won't work in other cases, e.g. file from BitTorrent, FTP. Full list of (11) supported apps in **`Exceptions.plist.`**
- Finder NOT protected (so copying Trojans from USB sticks isn't detected!).
- Trojans hidden within .mpkg files not detected.
- Not all variants of each Trojan detected, e.g. only 15 of 17 variants of RSPlug.

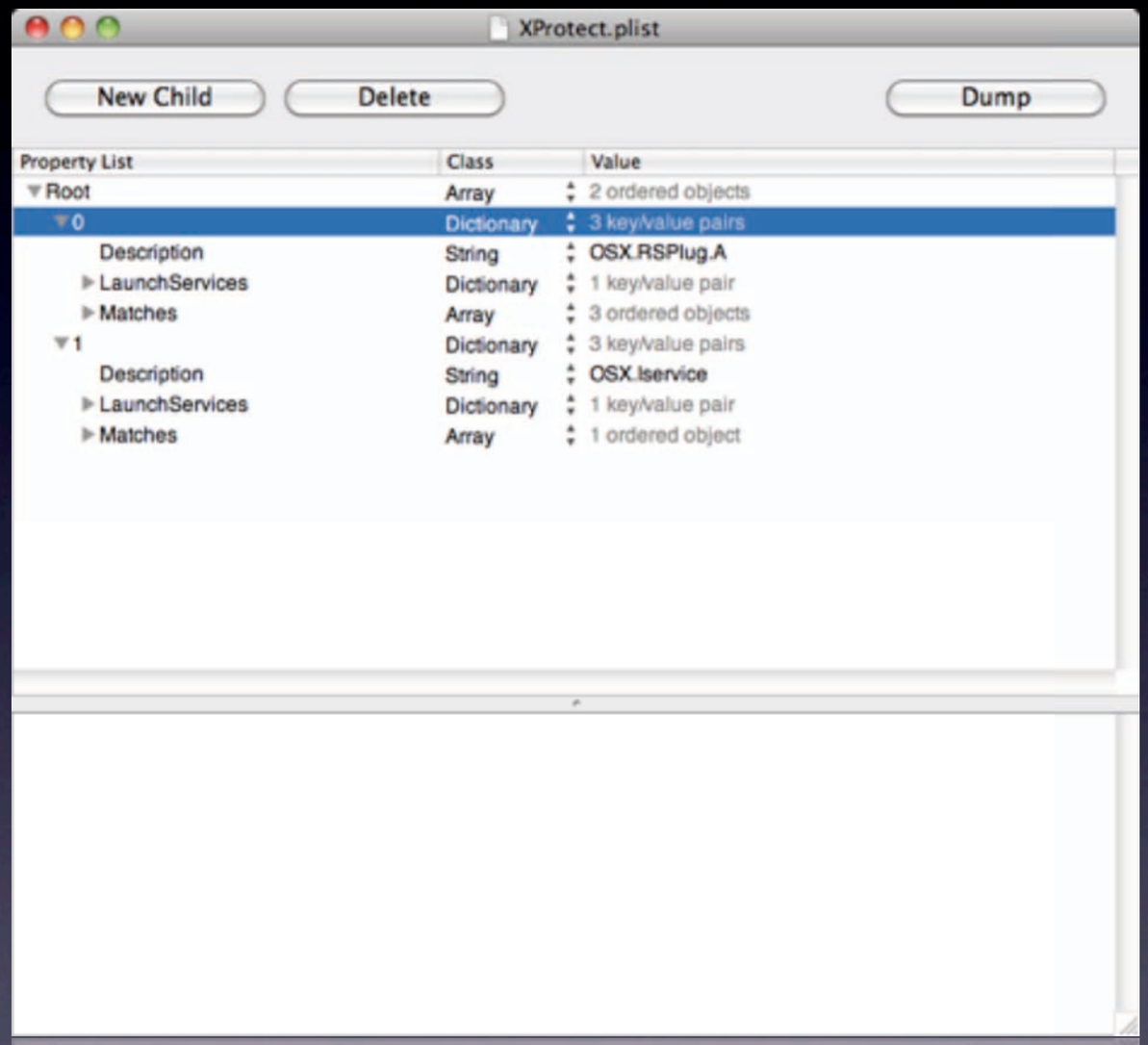
Quarantine

- Quarantined apps are checked for malware listed in: **`/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist`**
- Quarantine is only supported by some apps, e.g. browsers, Mail (& Thunderbird), iChat, Entourage. Won't work in other cases, e.g. file from BitTorrent, FTP. Full list of (11) supported apps in **`Exceptions.plist`**.
- Finder NOT protected (so copying Trojans from USB sticks isn't detected!).
- Trojans hidden within .mpkg files not detected.
- Not all variants of each Trojan detected, e.g. only 15 of 17 variants of RSPlug.
- List of "untrusted" file types maintained in **`System`** file in same directory. Just updated to include Safari Extensions (.safariextz).

Quarantine

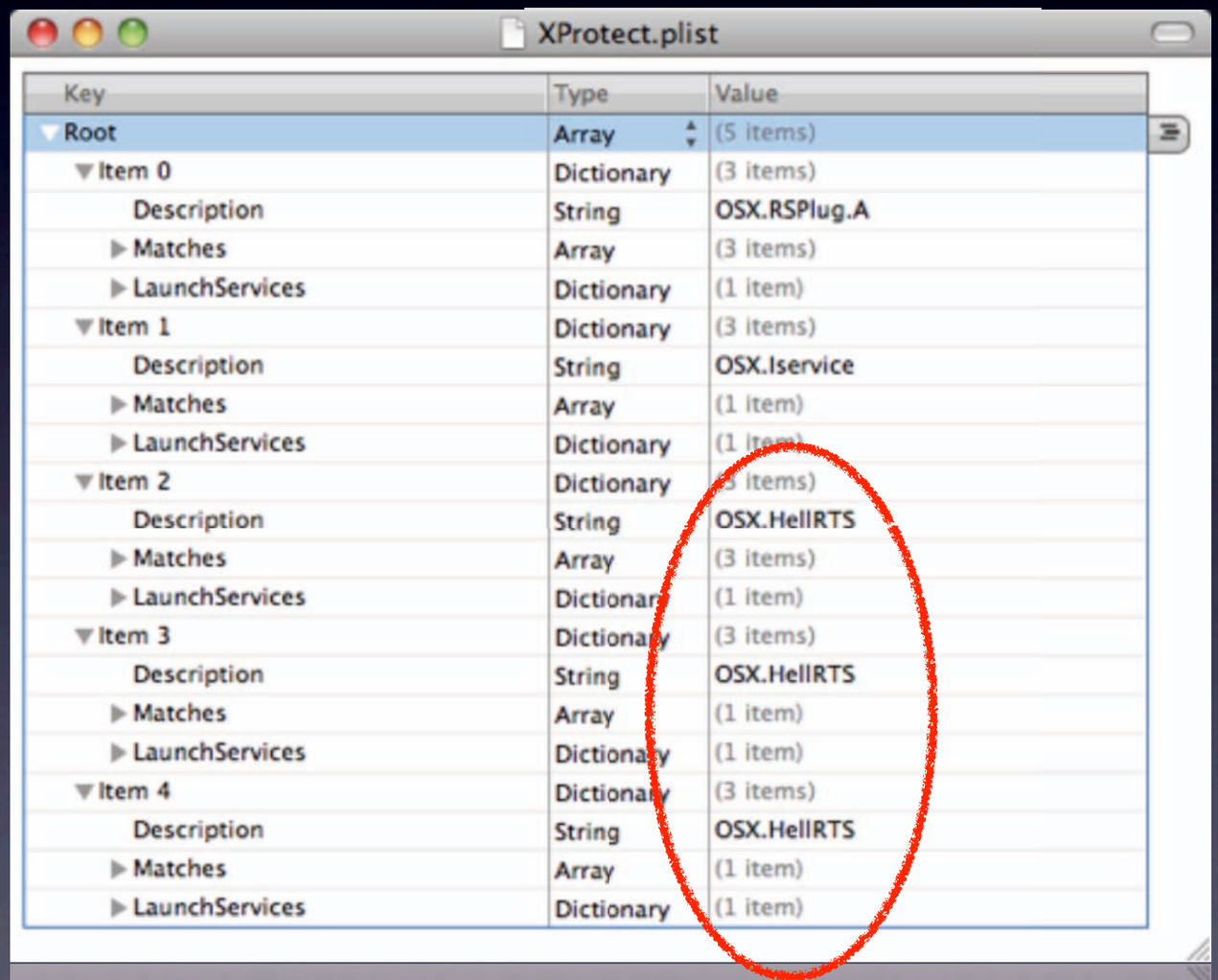
- Quarantined apps are checked for malware listed in: **`/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist`**
- Quarantine is only supported by some apps, e.g. browsers, Mail (& Thunderbird), iChat, Entourage. Won't work in other cases, e.g. file from BitTorrent, FTP. Full list of (11) supported apps in **`Exceptions.plist`**.
- Finder NOT protected (so copying Trojans from USB sticks isn't detected!).
- Trojans hidden within .mpkg files not detected.
- Not all variants of each Trojan detected, e.g. only 15 of 17 variants of RSPlug.
- List of "untrusted" file types maintained in **`System`** file in same directory. Just updated to include Safari Extensions (.safariextz).
- Malware definition update policy a little problematic: OS X 10.6.4 updated to include HellRTS but this not described in update notes or security bulletin.

/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist



10.6.3

10.6.4



Safari

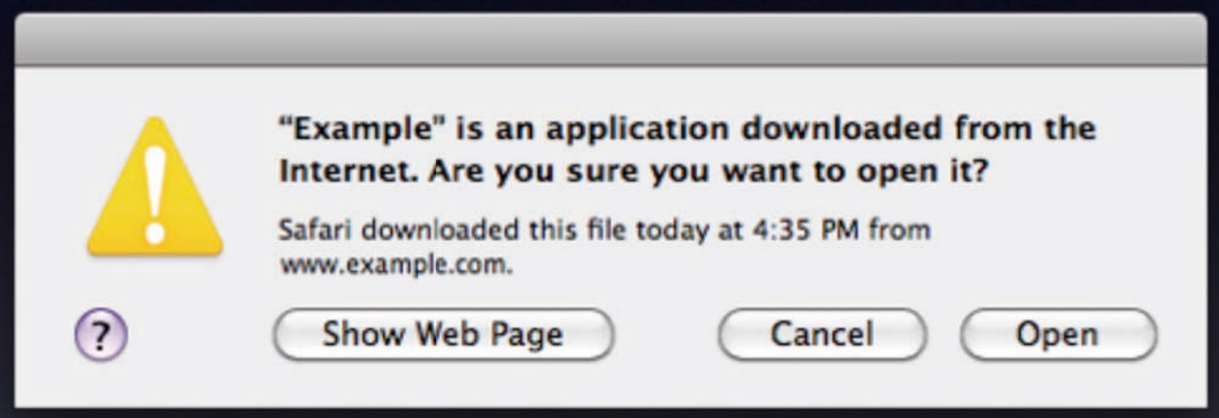
Downloads are quarantined

Anti-phishing (using Google blacklist of phishing sites)

Always disable Open “safe” files after downloading (in Safari > Preferences)

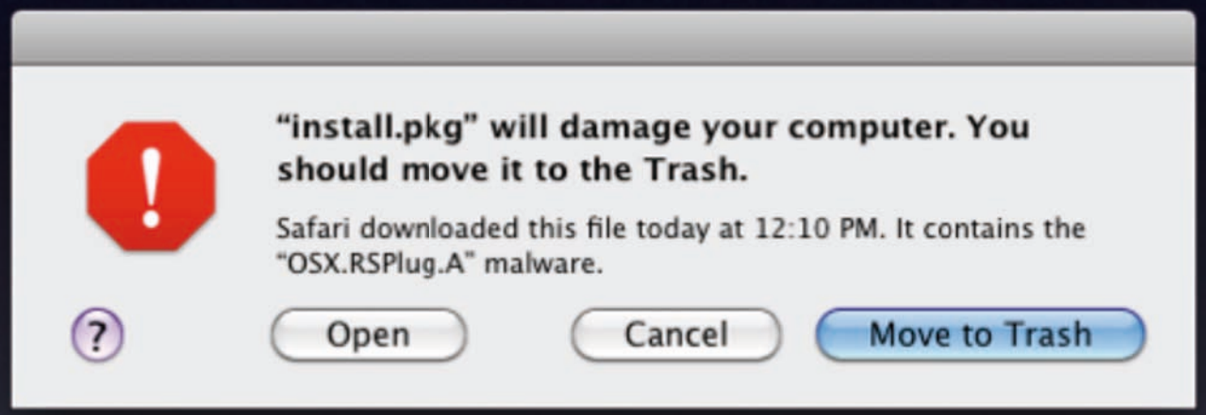
Safari

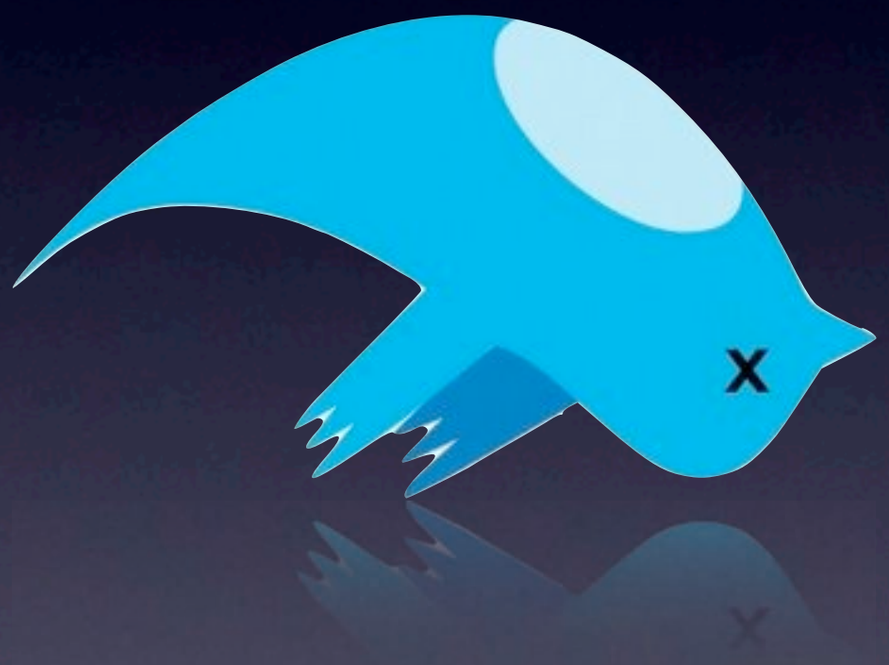
Downloaded apps are quarantined:



Safari

Downloaded apps are quarantined:





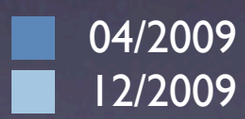
Social Media

Social Media

Social media & networks

There has been a rise of 70.6% in social network spam in 2009, with 69.8% malware being sent.

Facebook is probably biggest security risk followed by MySpace, Twitter and LinkedIn.

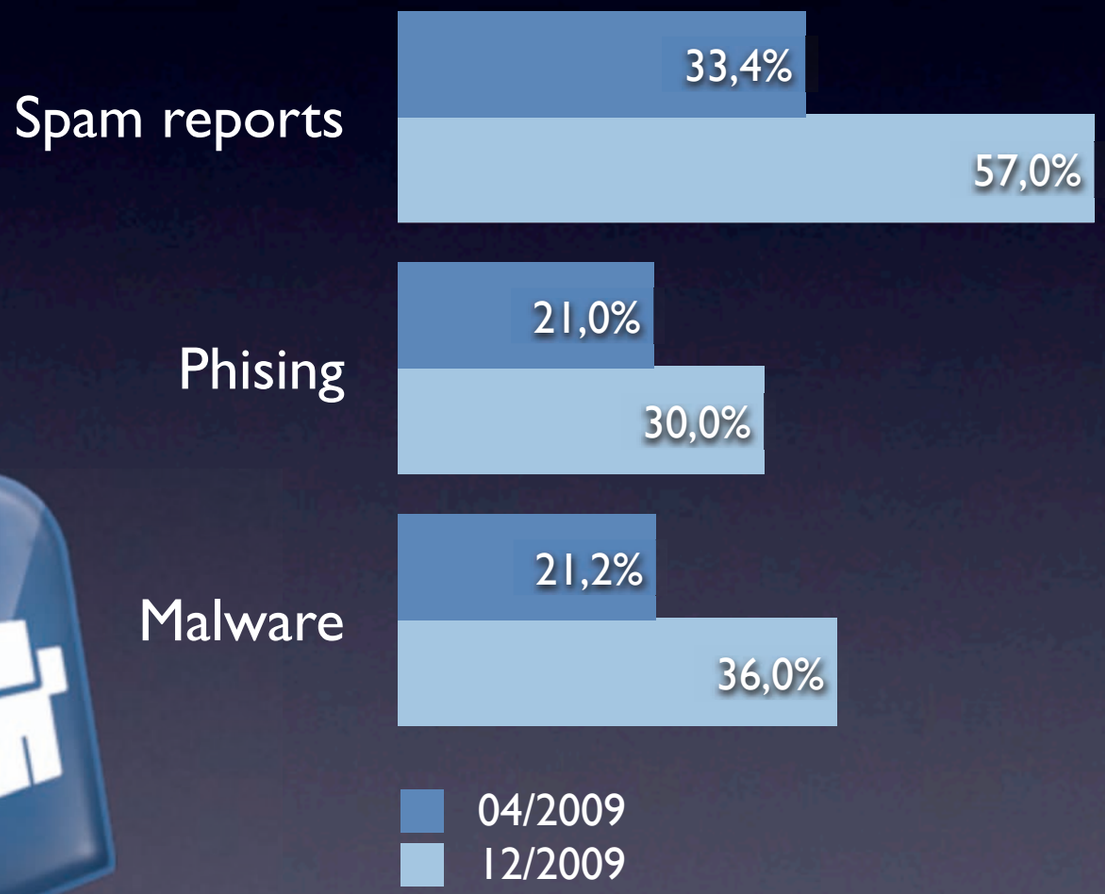


Social networks, Spam, Phising and Malware reports rising

Source: Sophos Security Threat Report 2010

Source: SC Magazine

Social media & networks



Social networks, Spam, Phising and Malware reports rising

Source: Sophos Security Threat Report 2010

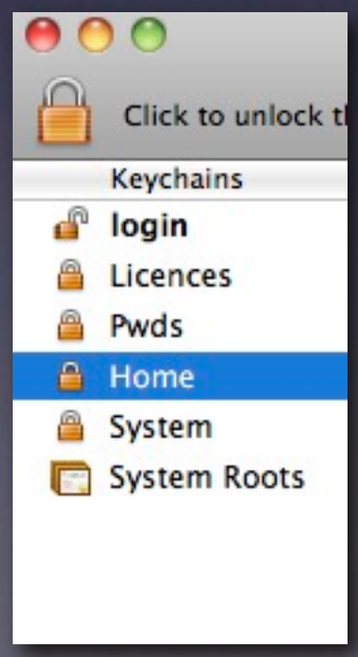
There has been a rise of 70.6% in social network spam in 2009, with 69.8% malware being sent.

Facebook is probably biggest security risk followed by MySpace, Twitter and LinkedIn.

Source: SC Magazine

Keychain Access

- A keychain is an encrypted container that holds passwords for multiple applications and secure services
- Triple-DES encryption
- Create additional keychains for specific uses



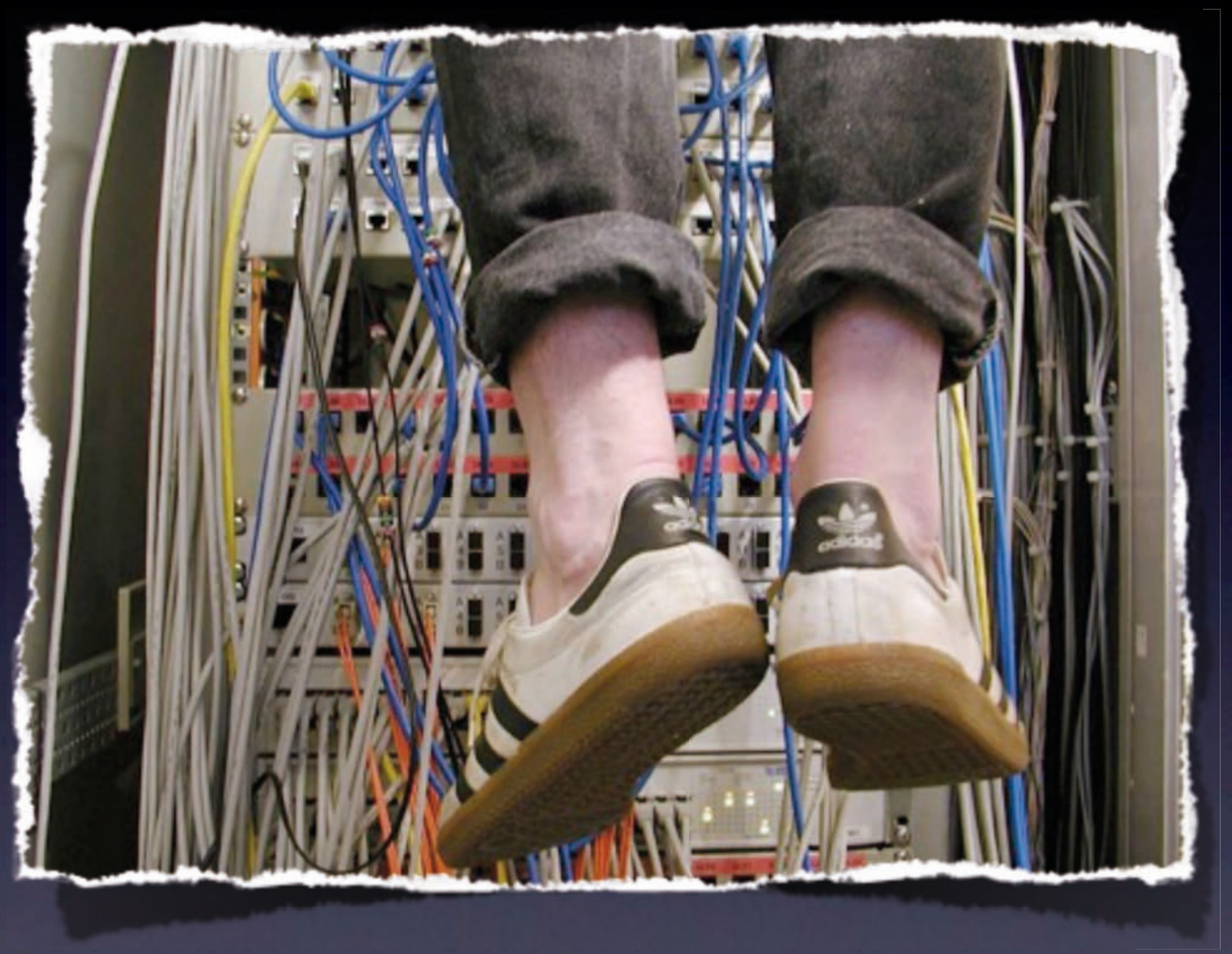
Further attack vectors

Further attack vectors

A **zero-day attack** is
a computer threat that tries to
exploit application vulnerabilities
that are **unknown** to others,
undisclosed to the software developer,
or for which **no security fix** is available.

Securing System Settings

- Securing System Prefs
  - Admin account: is it necessary?
  - What other prefs can be secured, and why?
- Securing Data
  - FileVault + alternatives
  - Always secure empty trash?
- Securing Applications
  - Application firewall (IPFW also available)



To be an Admin or not to be an Admin?

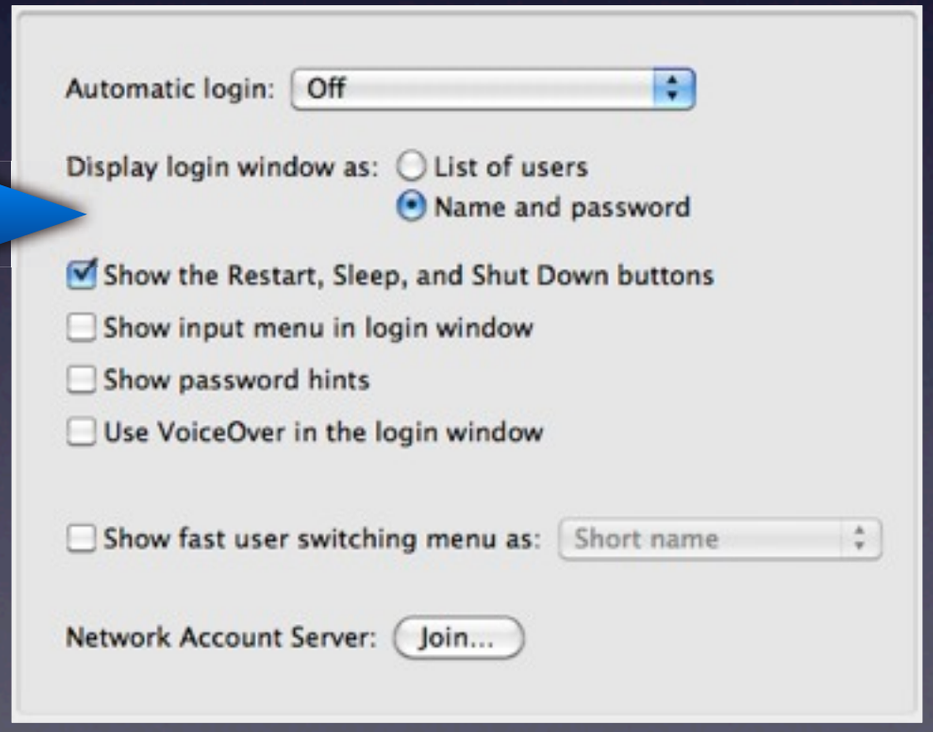
Hide Admin users from login window

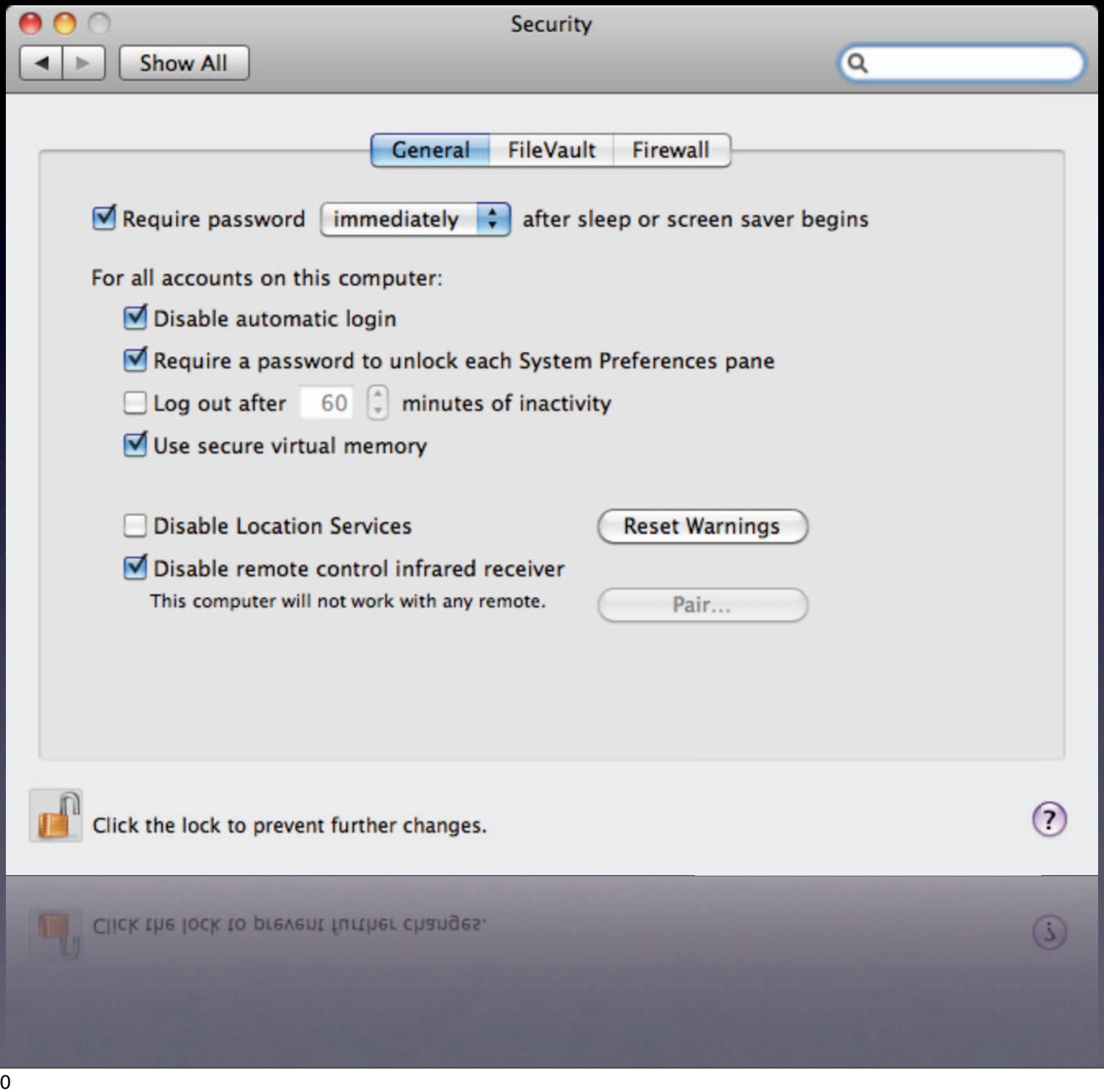
```
% sudo defaults write /Library/Preferences/com.apple.loginwindow
        HiddenUsersList -array-add [adminshortname]
```

Hide Admin users from login window

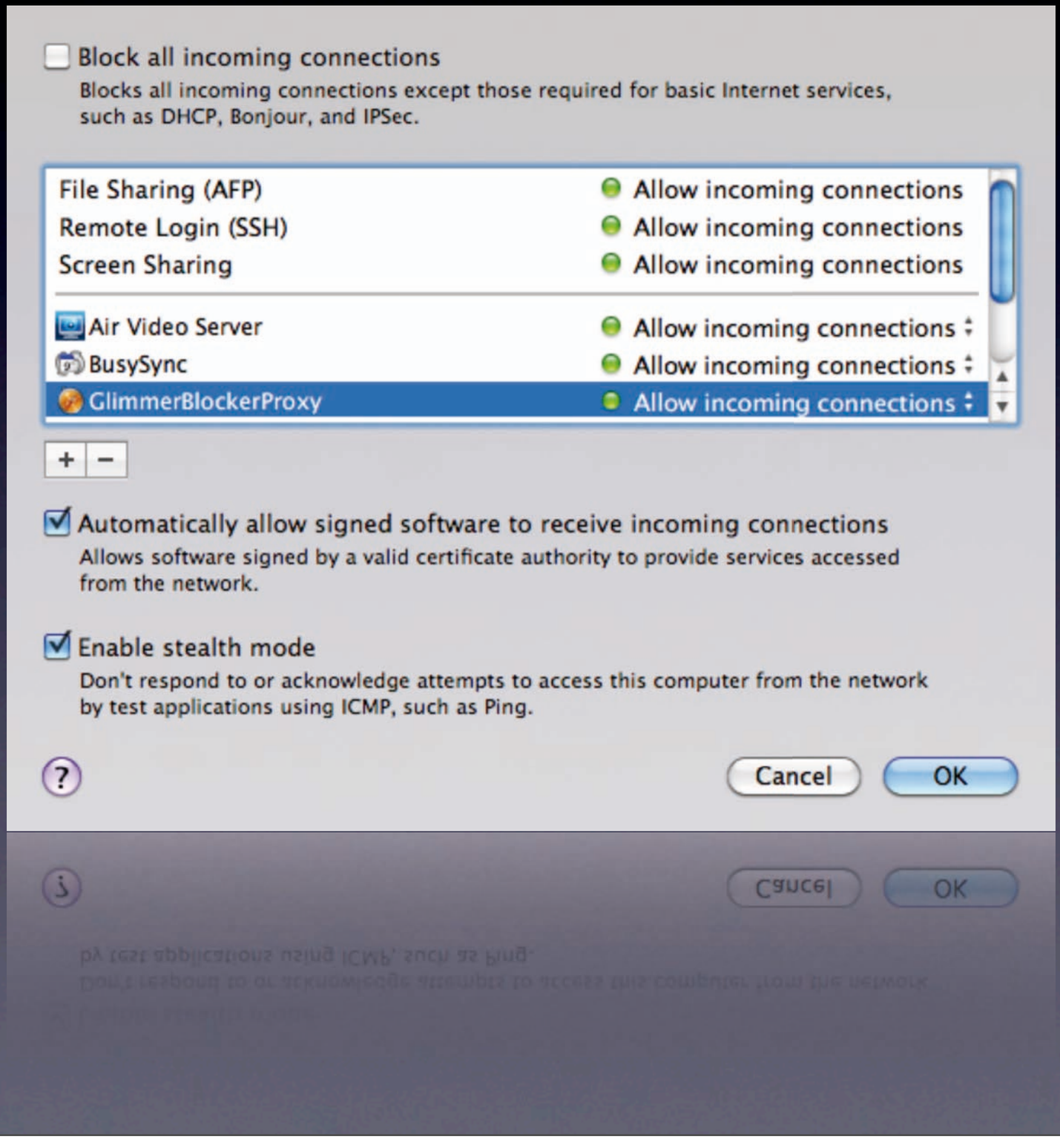
```
% sudo defaults write /Library/Preferences/com.apple.loginwindow
        HiddenUsersList -array-add [adminshortname]
```

And...

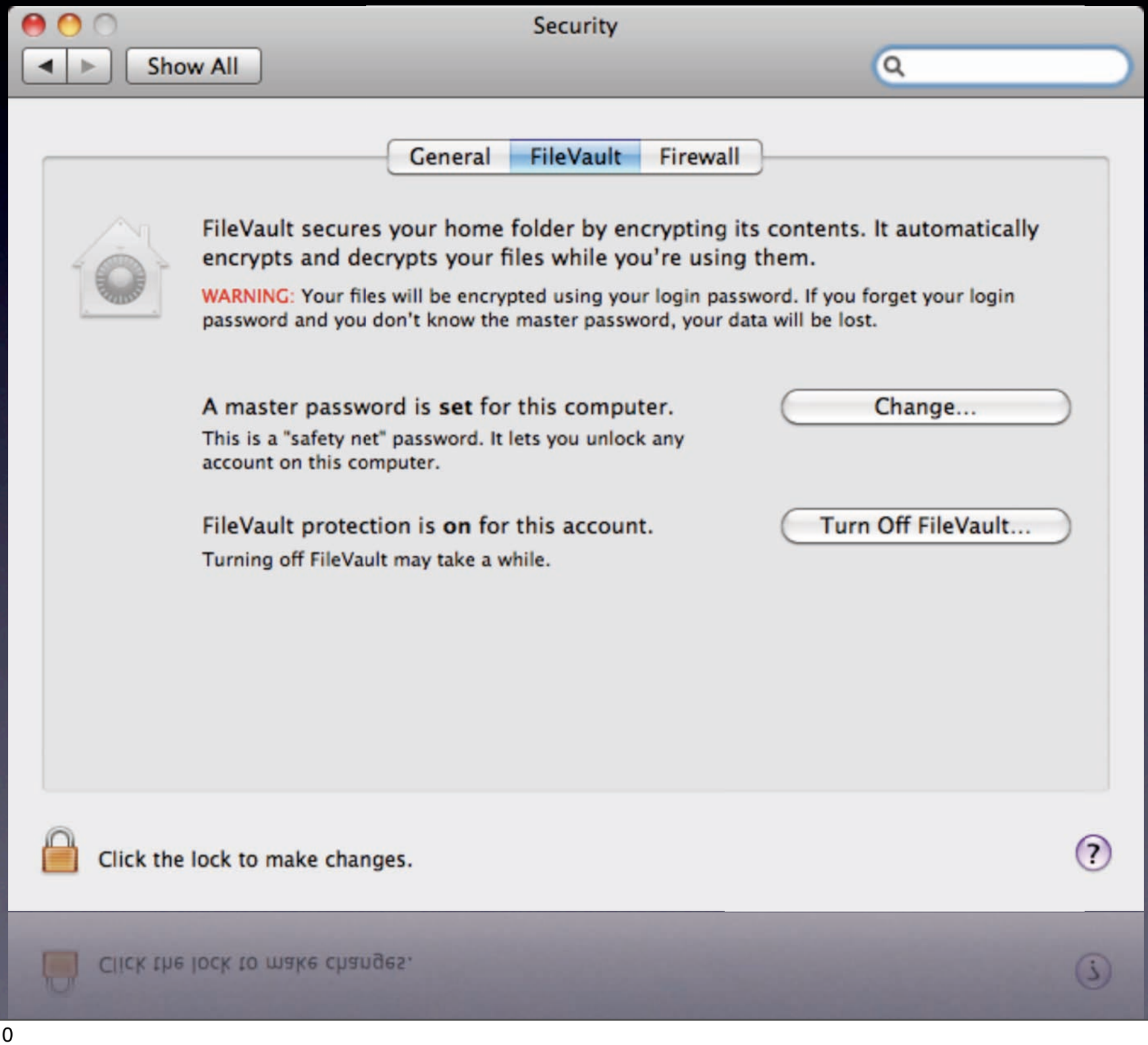



Security
Show All
General
FileVault
Firewall
Require password
immediately
after sleep or screen saver begins
For all accounts on this computer:
Disable automatic login
Require a password to unlock each System Preferences pane
Log out after
60
minutes of inactivity
Use secure virtual memory
Disable Location Services
Reset Warnings
Disable remote control infrared receiver
This computer will not work with any remote.
Pair...
Click the lock to prevent further changes.
?

Application Firewall



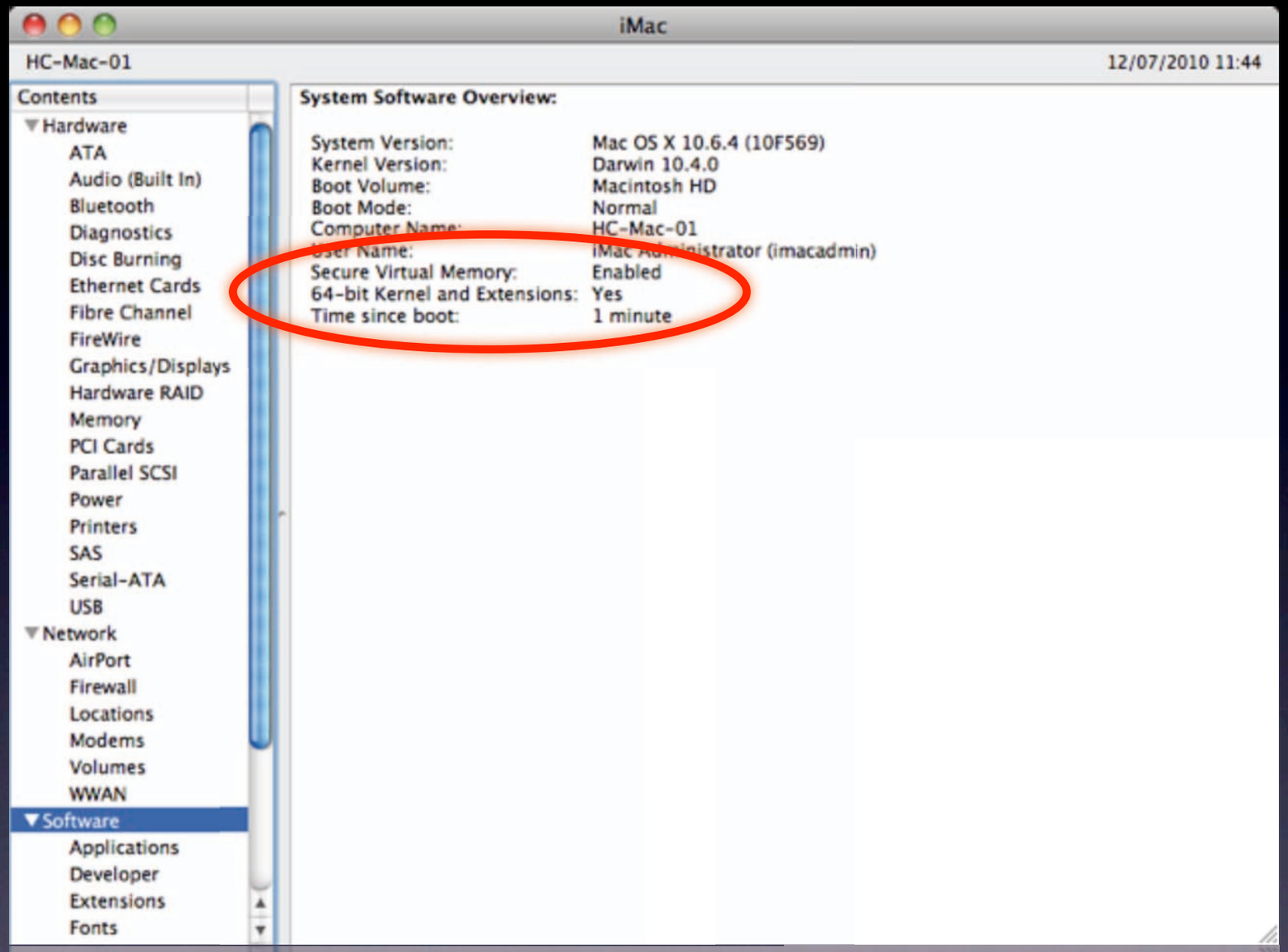
FileVault


Security
Show All
General
FileVault
Firewall
FileVault secures your home folder by encrypting its contents. It automatically encrypts and decrypts your files while you're using them.
WARNING: Your files will be encrypted using your login password. If you forget your login password and you don't know the master password, your data will be lost.
A master password is set for this computer.
This is a "safety net" password. It lets you unlock any account on this computer.
Change...
FileVault protection is on for this account.
Turning off FileVault may take a while.
Turn Off FileVault...
Click the lock to make changes.
?

- Use `hdiutil` to create encrypted folders from command line (or Disk Utility for a GUI)

- Third-party apps:
  - TrueCrypt <http://www.truecrypt.org/>)
  - Knox <http://agilewebsolutions.com/knox>

- PGP Whole Disk Encryption


iMac
HC-Mac-01
12/07/2010 11:44
Contents
Hardware
ATA
Audio (Built In)
Bluetooth
Diagnostics
Disc Burning
Ethernet Cards
Fibre Channel
FireWire
Graphics/Displays
Hardware RAID
Memory
PCI Cards
Parallel SCSI
Power
Printers
SAS
Serial-ATA
USB
Network
AirPort
Firewall
Locations
Modems
Volumes
WWAN
Software
Applications
Developer
Extensions
Fonts
System Software Overview:
System Version: Mac OS X 10.6.4 (10F569)
Kernel Version: Darwin 10.4.0
Boot Volume: Macintosh HD
Boot Mode: Normal
Computer Name: HC-Mac-01
User Name: iMac Administrator (imacadmin)
Secure Virtual Memory: Enabled
64-bit Kernel and Extensions: Yes
Time since boot: 1 minute


64
64-bit

64-bit kernel

64-bit kernel enabled Macs:
http://support.apple.com/kb/HT3770

64-bit kernel

64-bit kernel enabled Macs:
http://support.apple.com/kb/HT3770

- 64-bit binaries set all writable memory as non-executable

64-bit kernel

64-bit kernel enabled Macs:
http://support.apple.com/kb/HT3770

- 64-bit binaries set all writable memory as non-executable
- ‘return-into-libc’ attacks more difficult

7 Steps to Heaven

7 Steps to Heaven

✓ Weak passwords will undermine all security

7 Steps to Heaven

✓ Weak passwords will undermine all security

✓ Use a standard (not Admin) account

7 Steps to Heaven

✓ Weak passwords will undermine all security

✓ Use a standard (not Admin) account

✓ Secure settings in System Preferences

7 Steps to Heaven

✓ Weak passwords will undermine all security

✓ Use a standard (not Admin) account

✓ Secure settings in System Preferences

✓ Patching the OS

7 Steps to Heaven

✓ Weak passwords will undermine all security

✓ Use a standard (not Admin) account

✓ Secure settings in System Preferences

✓ Patching the OS

✓ Updating third-party apps

7 Steps to Heaven

✓ Weak passwords will undermine all security

✓ Use a standard (not Admin) account

✓ Secure settings in System Preferences

✓ Patching the OS

✓ Updating third-party apps

✓ Anti-malware software (up to date!)

7 Steps to Heaven

✓ Weak passwords will undermine all security

✓ Use a standard (not Admin) account

✓ Secure settings in System Preferences

✓ Patching the OS

✓ Updating third-party apps

✓ Anti-malware software (up to date!)

✓ Careful use of encryption

How We Do It?

com.apple.loginwindow

	Name	Apply To	Key Name	Type	Value		
ⓘ	autoLoginUser	User Level At Every Login	autoLoginUser	string	macuser	Edit	Delete
ⓘ	Disable Auto Login	System Level Enforced	com.apple.login.mcx.DisableAutoLoginClient	boolean	true	Edit	Delete
ⓘ	Background of Login Window	System Level Enforced	DesktopPicture	string	/Library/Desktop Pic	Edit	Delete
ⓘ	Guest User Login Window Warning	System Level Enforced	LoginwindowText	string	NSMS Managed Macinto	Edit	Delete
ⓘ	Login Display Text Entry	System Level Enforced	SHOWFULLNAME	boolean	true	Edit	Delete
ⓘ	Hide Shut Down Button	System Level Enforced	ShutDownDisabled	boolean	true	Edit	Delete
ⓘ	Disable Shutdown Apple Menu Item	User Level Enforced	ShutDownDisabledWhileLoggedIn	boolean	true	Edit	Delete

com.apple.screensaver

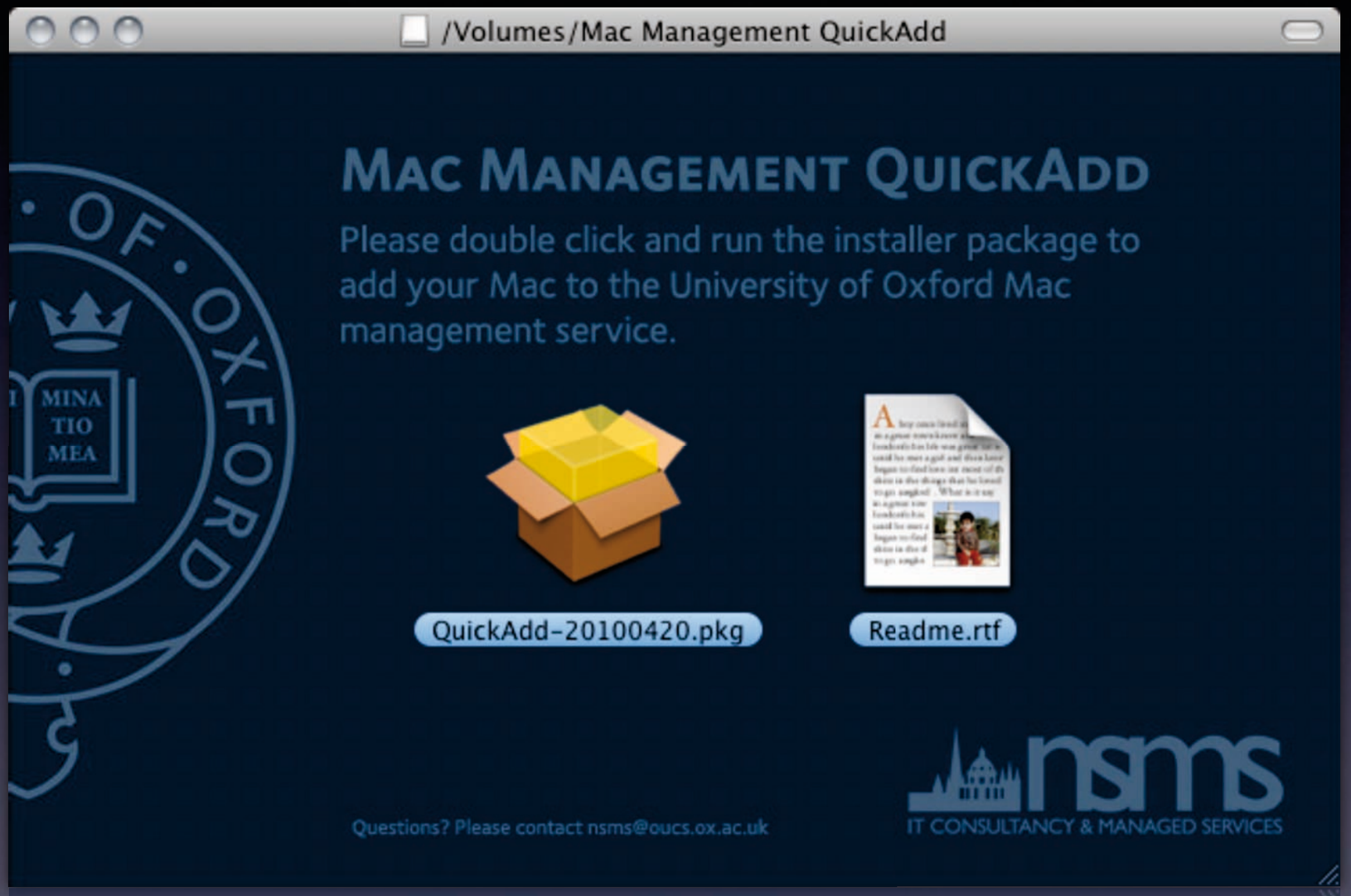
	Name	Apply To	Key Name	Type	Value		
ⓘ	Don't require password	User Level Enforced	askForPassword	integer	0	Edit	Delete

How We Do It?

OS	SWUs	Model	Sophos - Virus Definition Date	Sophos - Virus Definition Version					
Mac OS X 10.4.10	0	iMac G5			Details	Logs	Edit	Autorun	Delete
Mac OS X 10.5.7	2	Mac mini (Intel)			Details	Logs	Edit	Autorun	Delete
Mac OS X 10.5.8	8	Mac mini	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.3	3	MacPro (Early 2009)	2010-06-07 00:00:00	4.54	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.3	5	iMac Intel (Late 2009)	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.3	0	MacBook (13-inch Aluminum, Early 2009)	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	MacPro	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	1	MacBook (13-inch 2008)	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	iMac Intel (Mid 2007)	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	iMac Intel (Late 2009)	2009-12-07 00:00:00	4.48	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	MacPro	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	iMac Intel (Late 2009)	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete

How We Do It?

OS	SWUs	Model	Sophos - Virus Definition Date	Sophos - Virus Definition Version					
Mac OS X 10.4.10	0	iMac G5			Details	Logs	Edit	Autorun	Delete
Mac OS X 10.5.7	2	Mac mini (Intel)			Details	Logs	Edit	Autorun	Delete
Mac OS X 10.5.8	8	Mac mini	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.3	3	MacPro (Early 2009)	2010-06-07 00:00:00	4.54	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.3	5	iMac Intel (Late 2009)	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.3	0	MacBook (13-inch Aluminum, Early 2009)	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	MacPro	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	1	MacBook (13-inch 2008)	Not installed	Not installed	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	iMac Intel (Mid 2007)	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	iMac Intel (Late 2009)	2009-12-07 00:00:00	4.48	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	MacPro	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete
Mac OS X 10.6.4	0	iMac Intel (Late 2009)	2010-07-05 00:00:00	4.55	Details	Logs	Edit	Autorun	Delete


/Volumes/Mac Management QuickAdd
MAC MANAGEMENT QUICKADD
Please double click and run the installer package to add your Mac to the University of Oxford Mac management service.
QuickAdd-20100420.pkg
Readme.rtf
Questions? Please contact nsms@oucs.ox.ac.uk
nsms
IT CONSULTANCY & MANAGED SERVICES

Links

- Apple Developer Notes: <http://developer.apple.com/mac/library/navigation/index.html#section=Topics&topic=Security>
- Apple's Snow Leopard Security Configuration Guide v10.6
- Mac-virus blog: <http://macviruscom.wordpress.com/mac-virus/>
- File quarantine in 10.5 & 10.6: <http://support.apple.com/kb/HT3662>
- *National Vulnerability Database (NVD)*
- CVE database

Q & A