OFFICE FOR RESEARCH & INFORMATION TECHNOLOGY
UT University of Tennessee

Mac OS X System Hardening Guidelines for Faculty and Staff Desktops

“Qui non est hodie cras minus aptus erit.” (“He who is not prepared today will be less so tomorrow.”) - Ovid

Introduction

System security is important! If you ask the question, "*Who would want to break into this system or why would they want to?,*" the how and why of this line of questioning could fill volumes.

The "who" could be anyone whether they have legitimate access or not. The "why" is simple: free computing resources, access to data, damaging your system, embarrsing the university. A compromised system can quickly become a liability as it can affect the network or operations on other machines both locally and remotely.

System security is a critical issue for the safety of your computer, the data on it, and possibly, the other computers on the network. This process of increasing system security is called *system hardening*. It is not a one-time event; it is a dynamic and reiterative process. Security holes are discovered daily in operating systems and programs. A secure system today may not be secure tomorrow. Some precautions taken now will save you from problems later.

There is no "magic bullet" for securing a system. Every aspect of the system and its maintenance must be considered when securing it. Securing in layers while adding granularity at each level is the best approach. For example, physical security is one layer. An example of adding granularity to physical security is to use badge access to the area where a machine is located. Host security could be considered at the top layer. An example of granularity at this layer is making sure all unnecessary Internet services are off. One single mechanism cannot be relied upon for the security of a system. It should be looked at from every angle with all the pieces and parts taken into consideration.

Knowledge is Power

A simple but invaluable rule of thumb in the reiterative process of system security is to "know your machine": be familiar with its users, processes, files, etc. At UT the best resources to learn more about Mac OS X anad Mac OS X security are the Information Technology Security Group http://oit.utk.edu/infosec/ and MacVolPlace http://oit.utk.edu/macvolplace/. Information on security updates included in Apple's software updates can be found at http://www.apple.com/support/security/security_updates.html.

This document contains specific guidelines for establishing a secure Mac OS X computing environment for an individual's personal desktop. The document is meant to provide The University of Tennessee, Knoxville support personnel and all interested systems users with a systematic approach to establish and maintain secure systems. This document will be maintained and kept current according to accepted industry standards by the Information Technology Security Group (ITSG). Please note that all exceptions to this guide shall be submitted in writing to security@utk.edu. Any questions can be directed to the ITSG at security@utk.edu or 974-6555.

Step 1 - Protecting against outside attacks

Security risks can be broken into two types: physical risks and network risks First we will address those things you can do to reduce the risks to your Mac from attacks over a network.

Up-to-date Software

The first thing you need to do is make sure that Mac OS X and its applications are up-to-date with bug fixes and security updates. Apple has provided a means to automatically notify Mac OS X users of application and Operating System updates. The *Software Update* preference pane can modify this behavior and download and install software updates. The default configuration is to check weekly for updates. This should be changed to daily in this preference pane.

Setting Software Update to Run Daily

1. *Click on System Preferences--> Software Update (Tab)*
2. *Change the default "weekly" to "daily"*
3. *Quit System Preferences*

Anti-virus Software

This policy does not specifically identify or comment on anti-virus software. Anti-virus software is required according to the Universities Acceptable Use Policy (AUP) http://oit.utk.edu/aup/. The software can be found here https://antivirus.utk.edu/

Firewall Software

Firewall software is highly recommended for all systems, especially those with sensitive information. When you enable the personal firewall in Mac OS X, all inbound connections are denied except for those that you explicitly permit. If you enable a service, say Personal Web Sharing, that service would be allowed through but all those that are not checked would be blocked.

The Mac OS X personal firewall protects your computer from unauthorized access by monitoring all incoming network traffic. The personal firewall is based on ipfw, a technology that has stood up to years of real-world use in protecting the most mission-critical UNIX computers on the Internet. The personal firewall is integrated in the Sharing preference pane, with simple on/off checkboxes to enable protection. In addition, it can be customized for additional communication services, IRC, Gnutella, or other user-definable services.The firewall GUI can be accessed in the following manner:

Enabling the Firewal:

1. *Open System Preferences --> Sharing --> Firewall*
2. *Click on Start*
3. *Quit System Preferences*

For additional information regarding anti-virus software and firewalls contact the LAN and Desktop Support (LADS) group at (865) 974-9800.

Strong Passwords

While many system attacks take advantage of software inadequacies, many also make use of user accounts with weak passwords. In order to prevent this sort of vulnerability, "policies" or rules define what sort of account/password "behavior" is appropriate, and what auditing behavior is required. The OIT Password Policy can be found on the Information Technology Security Group web site at

http://oit.utk.edu/infosec/Password_Policy.htm

and is recommended for all systems at the University.

Mac OS X lacks the ability to force standard account/password complexity and maintenance rules found in other operating systems such as password length, composition, change frequency, lock-out threshold, etc. Therefore it is up to each individual to create and use STRONG passwords in line with the “OIT Password Policy.”

Step 2 - Physical Security

All systems analyst, support personnel, and system users need to be aware that physical security plays a role in the overall protection of each system attached to the University’s networks. Machine access should be restricted as much as possible. But in the event that someone has gotten into your office and now has physical access to your computer this document tells you what to do to make it difficult to impossible for the intruder to do gain access. Once again there is no “silver bullet.” But these steps should stop 99% of the population.

1. Screen saver password

A minimal requirement is to establish a screen saver password.

Enabling a Screen Effect (Same as Screen Saver)

1. *Click on System Preferences--> Screen Effect s--> Activation (Tab)*
2. *Set "Time until screen effect starts" =* ***5 minutes***
3. *Set "Password to use when waking the screen effect" =* ***use my user account password***
4. *Click on the Hot Corners (tab) and place a check mark in one of the corner boxes. This allows the user to move the mouse pointer to the corner of the desktop specified to launch the screen effect.*

2. Set an Open Firmware Password

Additionally, Open Firmware password protection (similar to a PC's BIOS password) should be used for systems that handle sensitive and/or business critical information. This setting is supported by Mac OS X 10.1 or later.

When you set a Firmware password, it prevents others from starting up the computer from a volume other than the one you have chosen as the startup disk (chosen in the Startup Disk preference panel within the System Preferences.) Once security is enabled, you cannot startup from other devices such as an external FireWire disk, a CD-ROM drive, or another partition or disk inside the computer.

It also offers additional protection against potential brute force attacks on the Open Firmware password by employing a progressive delay technique.
The delay itself increases in a pattern of 2 x N seconds (N = the login attempt number) between each invalid authentication attempt. The following process will configure the system to require the user to enter the Open Firmware password before the system will boot.
Download and Install the Open Firmware Password application,
http://docs.info.apple.com/article.html?artnum=120095
and run it. It will ask for a password or phrase. Be sure to use a "strong" password and be sure to remember it.

Enabling Open Firmware Password Protection:

1. Double click the application icon to open it.
2. Click the "Change" button to modify the security settings.
3. If you are enabling the security features, enter a password into the Password and Verify boxes.
4. Click the OK button.
5. Follow the prompts to enter your system administrator account.

You now cannot startup the computer from another device.

3. Set the Root User

Mac OS X, by default, has configured the root account to be disabled and has left the account with a blank password. As such, it the system were compromised, the root account could easily be enabled. Without the presence of a password, the attacker would have unlimited access to the system and its resources. To address this issue, the root account must be secured with a strong password. The following procedure illustrates the process.

Enabling/Disabling the root account

1. Click the Finder icon in the Dock.
2. Choose Go --> Applications (Applications from the Go menu).
3. Open the Utilities folder.
4. Open the NetInfo Manager utility.
5. Click the lock in the NetInfo Manager window.
6. Enter the name and password of an Admin user, then click OK.
7. Choose Security --> Enable Root User.
8. If you have not previously set a root password, an alert box may appear that says "NetInfo Error," indicating that the password is blank. Click OK.
9. Enter the root password you wish to use and click Set.
10. Enter the password again for verification and click Verify.
11. The root user is now enabled.
12. Choose Security --> Disable Root User

4. Disable Auto logon

A default installation of Mac OS X is configured to automatically logon the first administrative user that is created. In addition, Mac OS X, by default, displays all valid user names in the login windows. Also, after 3 invalid login attempts, by default, it will prompt the user with a password hint. This can provide easy access and/or useful information to anyone with physical access to the system. These features should be disabled on all systems.

Disabling Automatic Logins & Securing Login Screen Information

1. Open System Preferences-->Accounts-->User (Tab)
2. *Uncheck the "Log in automatically as ..." checkbox*
3. *Click on Login Options (tab)*
4. *Set "Display Login Windows as" = Name and Password*
5. *Unselect the "Show password hint after 3 attempts to enter a password" checkbox*

5. Do not dual boot

It is important that when you set up Mac OS X that you do not set it to boot into Mac OS X and into Classic (Mac OS 9) at startup. This creates a possible window of opportunity for an unauthorized person who might have physical access to your machine. If you are currently dual booting turn it off in

System Preferences -->Classic

Step 3 - Securing your data

Mac OS X v10.2 “Jaguar” has built-in applications that help protect your system and your data.

Encrypted disk images
The safety and privacy of your data is very important; this is of special concern for laptop users, who are at increased risk of computer theft or loss. Even if your Mac is stolen or lost, your encrypted data remains secure. The included Disk Copy utility permits users to create a disk image that’s protected with Advanced Encryption Standard (AES) 128-bit encryption. A disk image is a file that behaves exactly like another drive, where you can drag and drop files and folders that are then automatically encrypted. The encrypted disk image appears as a volume on your hard drive and can be copied, moved, or opened.

When you access the encrypted data via your chosen password or automatically with the keychain, the file is decrypted on the fly, meaning that it becomes readable only as your application needs it. For example, if you store a QuickTime movie in an encrypted disk image, only the part you are currently viewing is actually decrypted. Because on-the-fly decryption does not require the creation of temporary files, data security is enhanced. The encrypted disk image can be stored on the local system or on CD or DVD, emailed to friends and colleagues, or posted to a network file server.

With great effort there may be software that can get by this feature however this will take care of the 99.9%.

Securing your e-mail
Apple’s Mail.app provides solid IMAP support and since Mac OS X 10.2 it began supporting super-secure mail-reading protocols (SSL) that help to stop bad guys from nabbing your passwords. You should enable this on your Mail.app

Step 4 – More you can do

Use it or loose it
You can also remove programs, disable or not enable services that are not needed or used. Each application or service has the potential to contain a bug or security flaw. This is not likely, but you might consider removing or disabling all unnecessary programs and services. By default, a Mac OS X installation has all services the Internet super-server may launch disabled.

It is very important to understand that an improperly configured service can present a vulnerability that can bypass security measures. Thus, it is critical to understand what the function of each active service is. You should research the appropriate security measures for software applications and services installed on your system. For more information please see Additional Resources in the Appendix.

Step 5 - Prepare for an Incident

Finally you should prepare the system for an incident. Being prepared for something bad happening to your OS is very important. There are only two kinds of computer user: Those who have lost data and those who will.

Backups

The most important step is to backup you hard disk often and have more than one copy. The objective is to get back to "the way things were" as quickly as possible after a crash or incident. If you hate the thought of losing even a single word then you will have three complete backups of your entire hard disk on DVD-R discs (or some other media) – in three different locations (i.e., one in a safe deposit box, one at home, and one at the office.)

Backup your system regularly. Nothing can replace a backup for allowing you to recover from an incident.

But there's more. You may also want to back up your hard disk to an external FireWire hard disk, then back it up again to a second FireWire hard disk. Every day. And I back up my Home folder three times a day on top of that. All of these backups should occur automatically and in the background without any intervention from you.

For all but the simplest needs you'll benefit from a program that automates the backup process. A backup program lets you select the files and folders you wish to back up, then, only backs up files that have changed since your last backup session. I recommend Retrospect backup software from Dantz Development (http://www.dantz.com).

Set Network Time Synchronization

Additionally, it is recommended that you set synchronize the time on your Mac using the UT network time server. This enables file date/time stamp accuracy and event log precision. Mac OS X has a built-in time client.

Enabling the **Network Time** *Service:*

1. *Click on System Preferences-->Date & Time-->Network Time (Tab)*
2. *Check the "Use a network time server" checkbox*
3. *Enter "ntp.utk.edu" in the field*
4. *Click on "Set Time Now" button*
5. *Quit System Preferences*

APPENDIX

System Administrators only

Identifying a System Compromise
The information outlined in this step is for trained System Administrators only. It is sufficient for the general user to be aware of potential threats, to monitor the performance and functionality of your system, and to notify the ITSG if you see any unusual activities***. It is recommended that all general system users contact a qualified System Administrator or the ITSG prior to attempting any of the activities listed in this section of the Hardening Guide.***

While the actions outlined in this guide will dramatically increase system security, system vulnerabilities may exist. New security holes are discovered regularly, thus, preparing for the worst is critical. These steps should help to facilitate identifying a system compromise, allow for forensic analysis, and enable a timely recovery.

Aside from consistently watching for common indications of a system compromise (listed below), you should consider recording cryptographic checksums. By doing so you can establish a baseline of system binaries, application code, and data. This allows you to compare the current file system against a known reliable version. Md5app from enigmarelle http://www.versiontracker.com/dyn/moreinfo/macosx/12550 will let you do this.

1. A system alarm or similar indication from an intrusion detection tool
2. Suspicious entries in system or network accounting (e.g., a UNIX user obtains privileged access without using authorized methods)
3. Accounting discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which there is no correlation)
4. Unsuccessful logon attempts
5. New user accounts of unknown origin
6. New files of unknown origin and function
7. Unexplained changes or attempt to change file sizes, check sums, date/time stamps, especially those related to system binaries or configuration files
8. Unexplained addition, deletion, or modification of data
9. Denial of service activity or inability of one or more users to login to an account; including admin/root logins to the console
10. System crashes
11. Poor system performance
12. Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords
13. Port Scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts)
14. Unusual usage times (statistically, more security incidents occur during non-working hours than any other time)

15. An indicated last time of usage of a account that does not correspond to the actual last time of usage for that account
16. Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

The most commonly accepted cryptographic checksum used today is the MD5 algorithm, created by Ron Rivest of MIT and published in April 1992 as RFC 1321. To learn more about the MD5 algorithm (included with Mac OS X) visit one of the following websites:

RFC 1321:
http://www.landfield.com/rfcs/rfc1321.html

Additionally, commercial products such as Tripwire automate the process and provide a management interface for easy administration. Tripwire is available at http://www.tripwire.com.

Password Administration

The lack of any method to force the creation of strong passwords on Mac OS X requires administrators to use another proactive password-checking method: password cracking. This should only be performed with authorization, preferably written authorization, from someone with the authority to confer it upon an administrator. Many tools exist to perform password cracking. A fairly complete listing of these tools can be found at http://packetstorm.decepticons.org/Crackers/.

Forensic Analysis

Forensic Analysis is the process of unearthing data of probative value from computer and information systems. The IT Security Group is responsible for gathering data and identifying security improvements for all security issues. Thus, it is imperative to maintain the integrity of possible evidence. This includes log files, trusted cryptographic checksums, and information pertaining to system users/groups.

Hackers are ever increasing an ability to cover their trails. Log files are often deleted or modified to protect the identity of the intruder. Thus, measures to preserve the integrity of log files should be taken. Perhaps the best method is to use a remote logging software application that allows system logs to be stored on a remote system. The following list of actions will greatly increase the ability for investigators to pursue an intruder.

- Set proper permissions on log files
- Use a separate server to gather log files
- Make regular backups of log files
- Use write once media for log files
- Encrypt the log files

- Review log files on a frequent basis

Timely Recovery

Current system backups are an important resource during the recovery process. When forensic data has been obtained from a compromised system, it is recommended that the machine be rebuilt and the system restored using reliable backup tapes. It is important to know *when* a system was compromised (file/date time stamps) so that a reliable backup can be used to restore it. Restoring the root kit should not be part of the recovery process!

Networking: Built-in Communications security

Whether communications are taking place over wired or wireless networks, Mac OS X v10.2 “Jaguar” provides secure access to network resources and protection against hackers. SSH (SecureShell), SSL (Secure Socket Layer), sftp (secure file transfer protocol), TCP_wrappers and **Kerberos** are all built into OS X.

Mac OS X Kerberos Extras

While Mac OS X 10.2 (Jaguar) ships with most parts of Kerberos for Macintosh, it does not include support for CFM-based Kerberos-using applications (such as Eudora and Fetch), and the GUI Kerberos management application is located in a hard-to-find location.

The Mac OS X 10.2 Kerberos Extras installer will install the Kerberos CFM support library and make an alias to the GUI Kerberos Management application in /Applications/Utilities (the Kerberos application ships in /System/Library/CoreSevices). By default the installer will also install a sample configuration file (edu.mit.Kerberos) if one does not already exist, or you can choose a custom install to force install a new (MIT-based) configuration file.

If you have just upgraded from Mac OS X 10.1 to 10.2, you must install the Mac OS X 10.2 Kerberos Extras even if you had Eudora and/or Fetch working previously. The Mac OS X 10.1 Kerberos Extras do not work on Mac OS X 10.2 and you must upgrade them.

http://web.mit.edu/macdev/Development/MITKerberos/Common/Documentation/osx-kerberos-extras.html

Additional Resources

No One document can provide a complete guide to securing a Mac OS X system. Thus, the following resources are available for additional information regarding the theory and concepts behind this document.

The Center for Internet Security – http://www.cisecurity.org
The SANs Institute – http://www.sans.org
National Security Agency Security Recommendation Guides – http://nsa1.www.conxion.com
CERT Coordination Center - http://www.cert.org
Packet Storm - http://www.packetstormsecurity.org
Security Focus - http://www.securityfocus.com/
Rain Forest Puppy - http://www.wiretrip.net/rfp/
#RootPrompt.org - http://rootprompt.org/
Security Geeks - http://securitygeeks.shmoo.com/

AirPort 2.0.4: About Using AirPort With Point to Point Tunneling Protocol (PPTP) http://www.info.apple.com/kbnum/n107223

AirPort Wireless Communications: FAQ - Part 1 of 3 -- What kind of security does AirPort provide? http://www.info.apple.com/kbnum/n58414

AirPort: Turning On Access Control http://www.info.apple.com/kbnum/n58571

An Introduction to Mac OS X Security http://developer.apple.com/internet/macosx/securityintro.html

Apple - Mac OS X - Technologies - Security http://www.apple.com/macosx/technologies/security.html

Apple Open Firmware Password http://www.versiontracker.com/dyn/moreinfo/macosx/12932

Apple Product Security http://www.info.apple.com/usen/security/index.html

Apple Security Updates http://docs.info.apple.com/article.html?artnum=61798

Configuring Jaguar's Firewall http://www.macdevcenter.com/pub/a/mac/2002/12/27/macosx_firewall.html

DDÕs Ultimate Guide to Mac OS Security http://homepage.mac.com/macbuddy/SecurityGuide.html

Hide files from even the most experienced Mac user :-) http://www.osxfaq.com/tips/doe/index4.ws

Little Snitch http://www.obdev.at/products/littlesnitch/index.html

Mac OS X 10.1, 10.2: How to Set up Open Firmware Password Protection http://www.info.apple.com/kbnum/n106482

Mac OS X 10.2: How to Protect System Files Used by the Classic Environment http://www.info.apple.com/kbnum/n25422

Mac OS X 10.2: Issues With Kerberized Carbon CFM Applications After Upgrading to Mac OS X 10.2 http://www.info.apple.com/kbnum/n107156

Mac OS X Mail: About Secure Email Communications (SSL) http://www.info.apple.com/kbnum/n42827

Mac OS X Security http://conferences.oreillynet.com/presentations/macosx02/towns_leon.pdf

Mac OS X: About the root User and How to Enable It http://www.info.apple.com/kbnum/n106290

Mac OS X: How to Change Security for Your Keychain http://www.info.apple.com/kbnum/n61193

Mac OS X: How to Choose a Secure Password http://www.info.apple.com/kbnum/n106521

Mac OS X: How to Keep Network Computers Secure http://www.info.apple.com/kbnum/n61534

Mac OS X: How to Share More Than Public Folders http://www.info.apple.com/kbnum/n106224

Mission Lockdown - Get Smart With Security Tactics for Mac OS X http://osxfaq.com/Tutorials/lockdown/index.ws

Open Firmware Security - Introduction http://www.macosxlabs.org/documentation/firmware_security/intro.html

PGP: Protecting Security Information http://www.info.apple.com/kbnum/n113553

Princeton University: Macintosh OS X Security http://www.princeton.edu/~psg/unix/osx/osxsecurity.html

SecureMac.com http://www.securemac.com/

Security: Mac OS X and UNIX http://developer.apple.com/internet/macosx/securitycompare.html

Secure Mail Reading on Mac OS X http://www.macdevcenter.com/pub/a/mac/2002/03/19/secure_mail.html

Snort Mac OS X http://www.securemac.com/macosxsnort.php http://www.snort.org/

UCONN: Computer and Network Security Page: Macintosh OS X Security http://www.security.uconn.edu/macosx.html