Interested in learning more about security?

SANS Institute

Security Consensus Operational Readiness Evaluation

SCORE Security Checklist

Mac OS X 10.5 Security Checklist

Prepared by: Cory Steers, Eric Conrad
Authors:
Adam Gray – CISM
Andrew Korty – GCIA, GCFA
Charles Edge - ACSA, MCSE, CCNA, CCA, Security+
Cory Steers – GSEC, GCFW, GCIA, CISSP
Neil Fryer – GSEC, CEH

Contributors:
Eric Conrad – GPEN, GCIH, GCIA, GAWN, GSEC, GCFA, CISSP

Originally Written 11/14/06
Last Updated 10/26/08

Table of Contents

This document can be used as an audit reference, or as a system hardening document for Apple's OS X operating system. This document is limited to versions 10.5.* of OS X. Security is complex and constantly changing. In addition to this checklist, consult any Apple Documentation and other sources for securing OS X that may help cover gaps in this document. See the Reference Section of this document for a list of additional resources.

You should also monitor mailing lists and forums pertaining to OS X security. Security organizations like Secunia.com and sans.org have mailing lists that include vulnerabilities and other security bulletins for OS X.

You'll notice some of the text is in a different format. The format is:

▫ Perform this action

The purpose of this document is to be a checklist; however, explanations of recommended actions are included for clarity.

This document provides steps you can take to harden your OS X system, but should not be considered a "silver bullet" protecting you from all security issues. A unique aspect of the Apple user is that they're quite likely to run third party services (such as Rumpus, FileMaker Server, CommuniGate Pro, Now Up-to-Date Server and Now Contact Server, Kerio, etc) that invoke a listener. The reader will need to consult product vendor resources to determine the most secure implementation of these products.

OS X Security Architecture

This part of the document will be light on “checklist” activities. Instead, we'll just briefly describe some of the security related features of the architecture.

Unix Infrastructure

OS X is a hybrid of the Mach kernel and FreeBSD. The Mach kernel-BSD combination came from NEXTSTEP and the NeXT computer that Steve Jobs unveiled in the late 1980s. The kernel tends to be what sets each OS apart from one another. For example, GNU/Linux is commonly referred to as just Linux, even though Linux is just one piece of the GNU/Linux OS. It’s an important piece, but not useful without the GNU pieces. In this regard Mac OS X is very similar. It has a non BSD kernel with BSD userspace and support tools. BSD is what provides the model for much of the security we'll be covering in this checklist.

As of Mac OS X 10.5, Apple has attained UNIX 03 Certification.

Security Framework

Apple used Open Source Software (OSS) when creating Mac OS X. Several projects were leveraged to make up Mac OS X, including the Apache web server, MIT Kerberos, Samba, SpamAssassin and the Common UNIX Printing System (CUPS)..

Apple's stance on open source is simple and is becoming more mainstream in the IT industry, with SUN, Novell and others embracing the open source model in some form. Open source allows public scrutiny of application code, and therefore more secure applications. The open source community also has an established reputation for a short turn around time for developing security related patches and fixes, which Apple typically incorporates into Mac OS X fairly quickly. This helps keep Mac OS X secure, and provides for timely patching of bugs that arise from the open source packages deployed within Mac OS X itself.

Apple has designed their security around the Common Data Security Architecture (CDSA) model, developed by Intel. CDSA is a set of layered security services and a cryptographic framework that provide an interoperable, cross-platform infrastructure for creating security-enabled applications for client-server environments. CDSA covers the essential components of security capability to equip applications with security services that provide cryptography, certificate management, trust policy management, and key recovery.

CDSA defines a horizontal, four-layer architecture:

1. Applications such as Mail, Safari, iChat, Disk Utility, Keychain Access and other applications developed by Apple.
2. Layered services and middleware including the APIs used by the Applications listed above. An application programming interface (API) is a set of definitions of the ways one piece of computer software communicates with another. It is a method of achieving abstraction, usually (but not necessarily) between lower-level and higher-level software. These APIs include interfaces for Keychains, File Signing, SSL and Certificate Management.
3. Common Security Services Manager (CSSM) infrastructure Common Security Services Manager (CSSM) Cryptographic Services Manager. The CSSM has functions to create and verify digital signatures, generate cryptographic keys, and create cryptographic hashes.
4. Security Service Provider Modules, also known as Add-in Modules are third party and non-application items built using the APIs in the second layer of the CDSA. This allows for extensibility to the framework.

The CDSA is an open source framework, allowing it to closely parallel many of Apple's other initiatives for security and development and receive peer review from a larger audience than just Apple users. CDSA allows Apple and the community of third-party developers to architect software in a secure manner while still supporting the networkable features required for the modern applications of today and tomorrow. For more information on the CDSA model see the Intel CDSA site at http://www.intel.com/ial/security.

Types of User Accounts and Account Philosophy

With any type of account there are several general guidelines to follow in order to help maximize the security of the multi-user environment. Apple uses several types of user accounts on OS X. Account types include the guest account, administrator account (also known as root), administrator accounts, accounts managed with parental controls, sharing only accounts and standard user accounts.

The guest account, standard user account, the managed non-Administrator account, and the administrator account are all allowed to logon using the graphical interface. We'll talk more about the system administrator account (root) below but it is worth noting that when enabled it can also log on at the login window. As with most types of computer and network security the least privileges required for a given task should apply and with user accounts it is more critical than with almost any other aspect of the system. If an account does not need administrative privileges then that account should not have administrative privileges. Likewise, if an account doesn't need access to log into the system except through file sharing then that user should have a sharing only account.

Never share accounts. Shared accounts make it difficult to monitor and detect malicious activity. Malicious actions often go unnoticed and changes are often ignored by other users on a system. Shared accounts also harm accountability: there is no clear audit trail as to who performed a specific action.

Use a standard user account for daily operations. Administrator accounts should *only* be used for operations that require administrative privileges. Administrator privileges are required for tasks like installing software, running updates and configuring various settings in the operating system. When running as an administrator, malicious software could affect the operating system or applications. Malicious software is often not able to exploit a given system if the local user executing the code does not have sufficient privileges to install or change the configuration of the system. Administrator accounts should not be used for writing documents, checking e-mail or browsing websites. Administrators of systems should always keep the segregation of duties when dealing with administrator and user actions.

User IDs are another item to be concerned with. This concept is identical to other UNIX operating systems. The acceptable user ID range is 501 to 2,147,483,648. By default, new users on a system are assigned a number starting at 501. If multiple users are created on a system or are part of a shared network, be sure that user IDs are unique for individual users through the entire system. User Ids are the underlying component that is checked for rights and privileges.

Securing Administrator Accounts

The first account created on a new installation of Mac OS X is an administrative account. This allows the owner of the computer to accomplish many of the tasks that are often performed with a computer. This default setup should be changed. The first step is to create a new account for administration:

- Open the System Preferences application.
- Click on the Accounts icon to open the Account System Preference Pane.
- If locked, click on the padlock to allow changes and authenticate.
- Click on the plus sign to create a new account.
- In the drop-down list for New Account: select Administrator in the list of account types.
- Type in the name of the account you wish to use for administrative purposes.
- Type a password and the password verification.
- Click on the Create Account button.

The next step is to remove the administrative privileges from the user created during system setup. With the account administration program still open:

- Click on the account that was created during the install.
- Uncheck the Allow this user to administer the computer check box.
- This will prompt for a user name and password. Supply the username and password from the administrator account created in the last step.
- Click the open padlock icon to lock out further changes.

With these two steps done the first steps for separating privileges is complete. To emphasize this yet again, the new account with administrative privileges should only be used for administration and not day-to-day activities.

Next, create any accounts that will only have access to remotely log into the system for the purpose of sharing files. To create an account that cannot log into the desktop but can only log in to share files:

- Open the System Preferences application.
- Click on the Accounts icon to open the Account System Preference Pane.
- If locked, click on the padlock to allow changes and authenticate.
- Click on the plus sign to create a new account.
- In the drop-down list for New Account: select Sharing Only.
- Enter the name of the account you wish to grant sharing access to.
- Type a password and the password verification.
- Click on the Create Account button.

Part of what makes it possible to use Mac OS X with a non-administrator account, and yet still convenient to make administrative changes has to do with the way that Mac OS X allows and authorizes what it considers to be administrative tasks.

First, we have sudo – a standard in the Unix environment. This terminal command allows accounts to run commands as another account (usually root). For example, in the Terminal application, if you typed in "/sbin/reboot" you'd get an "Operation not permitted" message, and nothing would happen. If you typed in "sudo /sbin/reboot", you would be prompted for your password, and then if you are an administrator the system would proceed to reboot (by default, if you aren't an administrator, sudo will provide you with an error about your privileges and fail to execute the command). Sudo is controlled by the /etc/sudoers configuration file, and is a pretty simple configuration on OS X. Essentially, the root account (which is covered below) and anyone in the admin group (all of your administrative accounts) can run anything they want. By default, no one else can run anything. Sudo is capable of much more granularity than this. View the man page for sudoers for more information on customizing your sudoers file.

Apple has another mechanism for administrative tasks through the GUI. The system will prompt you for credentials any time you try to do something the system considers administrative. The ID and password of a valid administrative account will be required to perform that task. This allows you to be logged in with a non-administrative account, and temporarily escalate your privileges before you go back to doing non-administrative activities. Sudo has a 5 minute default cache, meaning that as long as you run a sudo command at least once every 5 minutes you aren't re-requested to authenticate. The GUI authentication mechanism has no such cache, so if you perform 3 administrative tasks within a 45 second time period, you will be prompted for credentials 3 different times.

This is similar to the runas command in Microsoft Windows 2000 and higher, but with a couple of key differences. First, in Windows you need to know that you need administrative privileges to do something and consciously right click on that action and select run as. In Mac OS X, you just perform the task as if you were the administrator and if administrator credentials are needed, Mac OS X will usually ask you for them.

Second, Apple has done a good job of identifying the tasks requiring administrative privileges. This is done in part within the context of the account property list files (plist files), file permissions and the sudoers file. If an item has privileges that your account cannot access then it can be accessed in this manner. As more applications for Mac OS X become available, applications that require credentials become a user's wakeup call that something is trying to make a change to their system.

Secure your administrator accounts, don't use administrator accounts for daily activity, and understand the two common ways to do administrative tasks on OS X and you will be well protected from Trojans and the accidental deletion of various files.

Also, if an account only needs access to a system via a network connection use a Sharing Only account. The Sharing Only account type does not authenticate through the login window and so minimizes the risk of unauthorized access to your system.

Finally, Parental Controls have been greatly improved in Mac OS X 10.5. Use a Managed with Parental Controls account in order to lock down certain features of Mac OS X. You can also build custom mcx files to further secure managed accounts. You can leverage the mcx framework by using the –mcximport extension of the dscl command. Using mcx it is possible to lock down nearly any feature of Mac OS X at the user or group level. An mcx can be set using Workgroup Manager and then imported through the dscl – mcximport command in much the same way you can set local policies in Windows using poledit, for example.

Groups

Groups were available in Tiger and below but have only been added to the Accounts System Preference pane in Leopard. Groups can be used to secure access to files and folders on the system.

To create a group:

- Open the System Preferences application.
- Click on the Accounts icon to open the Account System Preference Pane.
- If locked, click on the padlock to allow changes and authenticate.
- Click on the plus sign to create a new account.
- From the New Account: drop-down list select Group.
- Enter a name for the group in the Name field.
- Click the Create Group button.

Once you have created a group you will need to add users to the group. To do so:

- Open the System Preferences application.
- Click on the Accounts icon to open the Account System Preference Pane.
- If locked, click on the padlock to allow changes and authenticate.
- Click on the group you would like to add members to and check the box for each member in the Membership: field.

Securing Non-administrator Accounts

Non-administrator accounts have several options. The default user account has very few options for additional lockdown. It has rights to control printers, burn CDs/DVDs, change passwords, open the system preferences, and run any application on the system. You cannot use the Parental Controls feature of Mac OS X with an administrative account.

Each Managed with Parental Controls account has additional selections depending on the need. The ability to control e-mail, system options, chat, browse the web, and view dictionary items are all available for the Managed with Parental Controls account. These items can be controlled via the Parental Controls System Preference pane. When parental controls are enabled the user is changed from a Standard User to a Managed with Parental Controls account.

In Mac OS X 10.5 you can now manage parental controls from a remote system (that is also running Leopard). To enable Parental Controls to be managed from a separate system:

- Open the System Preferences application.
- Click on the Parental Controls icon to open the Parental Controls System Preference Pane.
- Check the box for Manage Parental Controls from another computer.

To manage Parental controls for an account:

- Open the System Preferences application.
- Click on the Parental Controls icon to open the Parental Controls System Preference Pane.
- Click on the user who you would like to setup parental controls for.
- Click on Enable Parental Controls.
- Set the Parental Controls for the account in question (see list below).

Parental Controls include the following:

System

The System tabs allow you to customize several items that control access to local resources. The Simple Finder restricts changes to the dock and only allows applications to be run that are part of the applications folder. Simple Finder also restricts users from using shortcut keys such as Command-C to copy files. Simple Finder also puts a user into a sandboxed environment graphically. The Simple Finder selection is important to use if users are not trusted or require very strict operating environments.

- For users who should not have full system access enable the SimpleFinder.

The Allow only selected applications: section allows you to restrict the applications that a user has access to. When you check the box for restricting Applications you will then need to check the box for each Application and Widget that a user will have access to.

- Allow Managed users to only have access to applications that are required.

The bottom of the System tab allows for more granular control over other components of the system. This can give you a full Finder menu while still allowing for control over items that include CD/DVD-burner capabilities, change password, administration of printers and whether a user is able to modify the dock.

- Disable features users should not have access to.

Content

The Dictionary control blocks access to certain types of words within the dictionary. This is mostly related to items containing profanity and drug related information. This can be done by simply clicking the check-box for the Hide profanity in Dictionary but does not allow for more granular controls at this time.

- Consider using the dictionary to limit access to inappropriate material.

The Website Restrictions control allows administrators to control access to web sites that a managed user can access through Safari. The Website Restrictions feature does not pertain to Firefox or other third party web browsers.   There are three settings for Website Restrictions. The Allow unrestricted access to websites setting places no restrictions on the user. The Try to limit access to adult websites automatically setting allows the system to automatically block certain sites and allows the administrative user to customize sites that are always and never blocked. Finally, the Allow access to only these websites feature allows you to allow only certain sites to be accessible.

- Block inappropriate sites for managed user accounts.

Mail & iChat

The mail security tab allows for configuration of e-mail permissions. This allows the administrator to review the inbound and outbound permissions on email. The iChat controls are very similar to the mail control. This allows an administrator to control who a managed non-Administrator account can chat with. Mail settings are only applied to Mail.app and iChat settings are only applied to iChat. Neither can be used to control 3rd party applications such as Entourage or AIM.

Communications are restricted for both iChat and Mail.app if each setting is enabled. The easiest way to allow access is to add users to your Address Book using the Address Book application and then select the users that can be communicated with within the Parental Controls Preference pane based on Address Book entries.

- Set the permissions on email and iChataccess. Add all users who a managed user should be able to communicate with.

You can also use the Send permission requests to: feature to enable the managed user the ability to email you with requests to add new users that can be communicated with.

To reiterate, the –mcximport extension of the dscl command can be used to import mcx settings at the group level. See the help section for the –mcx* extensions of dscl for more information on how to set these up.

Securing the System Administrator Account

Not to be confused with *an* administrator account, *the* system administrator account is the account with UID 0 and a shortname of root. From here on, this document will be referring to this account as root, or the root account. By default, root is disabled in OS X client but enabled on OS X Server. This is a good thing on OS X Client, as this account has full privileges to do anything on the system. As already discussed in this section, OS X has a more restricted and complex method for administration. Root reduces that complexity and granularity to simply provide administrative access.

Note: User and group management is different in Mac OS X than in a standard Unix environment.
In Mac OS X 10.5 and above Apple migrated to storing account information in property list files, similar to an /etc/passwd file but with each account having their own file. This includes service accounts, signified by having names that start with an underscore (_) and user accounts. User accounts are located at /var/db/dslocal/nodes/Default/Users. Groups are located at /var/db/dslocal/nodes/Default/Groups. You can delete unused accounts by removing them from the directory structure or by using the Accounts System Preference Pane. You can also redirect a users home folder, restrict shell access, change short names, change UIDs and change default groups (eg – for umask) using these files (although you should do so with caution), Service accounts, by default, do not have passwords associated with them. You can assign a password to a service account using the –passwd extension to the dscl command.

In Mac OS X the shadow directory is located in /var/db/shadow/hash. In this directory you will find the encrypted password hashes for any accounts with a password associated with them. The accounts are listed with the GeneratedUID as the naming convention. To find the GeneratedUID for any account you can use dscl to read the account property list.

A disabled user may not mean the same thing as in other operating systems. In the Mac OS X context, disabled means that another account has to be privileged (essentially root) to use the account. Disabled accounts are still defined and root uses disabled accounts all the time to run background processes. Most application-oriented accounts like apache, sshd, and mysql are disabled with no password defined and no way to switch a non-root user to them.

While direct root access is limited on OS X, the kernel starts launchd as root during boot up. If you're a UNIX aficionado, you can relate launchd to init (although Mac OS X uses init as well, it should not be used so as not to have software updates overwrite your additions to init). Most UNIX distributions use init, and earlier versions of OS X did as well. Root also owns files with the Set User ID (SUID) bit turned on (SUID is explained further in the File Permissions section). Accounts with permission to execute SUID files execute them with the authority of the owning user. This explains how sudo and Mac OS X's GUI authorization prompt work.

Apple provides a way to administer OS X without becoming root, and allows you to do things as root using sudo. When root is disabled, an attacker is unable to gain root privileges by brute forcing root's password, because the password doesn't exist and no mechanism to log in as root exists. If root is enabled then it is possible to attempt to guess the root password, or change it by booting a computer to a CD and resetting the password.

It is recommended to leave root disabled. But if you need to enable it (and you likely will to do some of the tasks in this checklist) it can be done by:

- ▫ Open Directory Utility by going to Applications/Utilities.
- ▫ If the padlock at the bottom left is closed, click on it and provide administrator credentials to unlock it.
- ▫ Click on Edit in the Toolbar.
- ▫ Click on Enable Root User in the Edit menu.
- ▫ Click the open padlock at the bottom left to re-lockout changes.

Note: If root is enabled, and you want to disable it, follow the same steps above, only the option under Security will be Disable root User. The root account should be disabled when it is not required.

Note: Whereas root itself may be disabled you can still use sudo bash to gain a privileged session while in Terminal.

Software Installation

Installing software can be dangerous provided you do not obtain your software from a trusted source. Therefore, Mac OS X 10.5 provides digital signing for all software installed. Additionally, when software that is obtained from the Internet is run for the first time you will now be prompted with a dialog box that states what site the software was obtained from and you must specifically allow the software to then be able to be run.

- ▫ Verify the digital signature on all software that is being installed on your systems against that of the vendor of the software.
- ▫ Check that you did indeed download software when using software that was downloaded from the Internet.

Much of the behavior of Mac OS X is controlled by options in the System Preferences. Only the System Preferences that impact security are described in this section.

To increase the system preferences security:

- Select System Preferences… from the Apple menu or open the System Preferences application from the /Applications folder.

At the array of icons each represents a different category of System Preferences. Each of the subsections below corresponds to one of those categories. Click once on an icon to bring up its preference pane. To get back to the menu:

- Click the Show All button at the top of the window.

Appearance

To prevent unauthorized access to recently-accessed applications, documents, and servers:

- Set Number of Recent Items to None for all Applications, Documents and Servers.

A locking screen saver can be used to reduce the risk of an intruder accessing the console of an unattended computer (see the next section). To avoid accidentally disabling the screensaver, make sure no hot corners are set to do so. To enable quickly putting the computer to sleep so it's locked:

- Setup a hot corner to put the computer to sleep.

Desktop & Screen Saver

A screensaver with 'require a password' (as indicated in the **Security** section below) can prevent unauthorized access to the desktop. If you install Check Point Full Disk Encryption the screen saver for Check Point will automatically be enabled.

- On the Screen Saver tab, select a screen saver that does not reveal information on or about the computer (for example, avoid Computer Name, Pictures Folder, or Choose Folder...) and leave Use random screen saver unchecked.
- Set Start screen saver to 10 minutes or a value consistent with local policy.
- Use Security System Preference Pane to require a password to wake from a screen saver (see below).

Security

For the FileVault section of the Security Preferences, refer to the Securing the System and the Data/Encrypting Home Folders section of this checklist.

To reduce the risk of unauthorized desktop or System Preferences access

- Check Require password to wake this computer from sleep or screen saver.
- Check **Disable automatic login** to require all users to authenticate before accessing the desktop.
- Check Require password to unlock each System Preference pane.
- Check **Log out after 60 minutes of inactivity**, substituting for **60** an appropriate number of minutes based on your local policy.
- Check **Use secure virtual memory** to prevent tampering and unauthorized access to

the memory space of running applications.

By default any infrared receiver can invoke the Front Row application on a Mac with infrared built in. On systems with infrared receivers, it is possible to reduce the risk of the system being controlled by unauthorized of infrared receivers, you should either use the Pair button of the Security System Preference to restrict the use of one infrared receiver that you have paired with the system. You can always unpair and switch receivers.

- Check Disable remote control infrared receiver.

The Firewall tab of the Security System Preference pane lets you configure the Mac OS X built-in application level firewall but not the command line ipfw firewall that was used in Tiger and below. The firewall in Mac OS X 10.5 works using application signing. When you enable the firewall only signed applications are capable of communicating with hosts outside your system. By default all internal communications for Apple services are signed. Every application that is installed is signed and various attributes are tracked. By default the firewall is disabled.

Note: Mac OS X Server has an improved interface for configuring the firewall and/or *ipfw*. See the **Mac OS X Server specific** section for details. If you are using Mac OS X Server then the Firewall tab will not be present in the Sharing System Preference.

If you use the built-in Firewall tab in the Security System Preference pane:

- Enable the firewall by choosing either the Allow only essential services (which enables only Apple services) or the Set access for Specific Services and Applications
- If using specific services add third party packages to be allowed
- Click on the Advanced button
- Check the box for Enable Firewall Logging (if you want to log traffic)
- Check the box for Enable Stealth Mode (if you do not want the system to respond on ports that are not opened).

Sandbox

The sandbox facility was added to Mac OS X 10.5 to help limit resources that a process has access to. Using sandbox you can implement Mandatory Access Controls, which allow you to limit what access that processes, sockets and threads have to files, folder, sockets, ports and memory. The sandbox facility can limit this access and provide a more granular approach to securing a system. Access to resources can now be doled out more granularly than can be within the confines of the POSIX file system.

- Test and implement sandbox in your servers and images where appropriate.

Spotlight

Spotlight indexes files on Mac OS X to speed up searching. These indexes could be another way to find sensitive information on your computer. However, by disabling Spotlight you remove one of the more popular features of Mac OS X so be wary when doing so.

- For maximum security, include all attached storage devices, including the internal hard drive, on the Privacy tab.

CDs & DVDs

Removable media may contain malware that, when automatically executed by the computer, infects or compromises it.

- To prevent the computer from automatically running anything when a CD or DVD is inserted, change all settings to Ignore.

Energy Saver

Often an attacker will attempt to reboot a computer to change security settings or in hopes that existing security settings won't be present on reboot.

- Uncheck both Restart automatically options to disable two ways an attacker could have an effect on a reboot. These options could, however, result in a denial of service because the system will be down until an administrator is able to attend to it. System maintainers should weigh the risks of each and configure the settings accordingly.

To prevent an attacker from waking up a sleeping computer via the network or modem:

- Uncheck both Wake Options.

It is easy to put a computer to sleep if you have physical access to the system. In data center environments this could result in an easy denial of service for users attempting to access web sites and other confidential material. To disable this feature:

- Uncheck Allow power button to sleep the computer.

Print & Fax

By default no printers are shared. You can enable Printer sharing per printer. By default printer and fax sharing is disabled. To only share printers that are required:

- Uncheck each printer that should not be shared.

The Mobile Me System Preference controls the computer's ability to synchronize files or other content with a Mobile Me account. To avoid sharing data in this way:

- Uncheck Synchronize with Mobile Me on the Sync pane and disable iDisk synchronization on the iDisk pane.

Your iDisk is synchronized with the Apple WebDAV servers. Many people use this option to transfer files. If you want to share files that are stored on your iDisk the permissions and access to these files can be set using the Mobile Me System Preference. To customize this:

- Click on the iDisk tab of the Mobile Me System Preferences.
- Check the box for Password protect your Public Folder.
- Use the Set Password (looks like a key next to the password field) button to set a strong password.

- Choose whether you want public users to have access to Read only or Read and Write data from the iDisk.

Note: If you have a Mobile Me account then you can download and use Apple's Backup application to back files up to your Mobile Me account or another hard drive. This gives you a low cost backup solution that is capable of backing files up in a way that preservers their unique attributes. You can also use time machine to backup your important files to a local or wireless hard drive.

Back to My Mac is a service that allows the use of file sharing and screen sharing of your Mac from another Mac over the Internet or an internal network. This service should be disabled.

To disable this:

- Click on the Back to My Mac tab of the Mobile Me System Preferences.
- Check the stop button. It will prompt for your password enter the administrator name and password and click ok.
- To customize this service if it is going to be run click on the Open Sharing Preferences button in the Back to My Mac tab of the Mobile Me System Preferences.
- Choose the specific services you would like to share such as file sharing or screen sharing.

To customize this:

- Click on the Back to My Mac tab of the Mobile Me System Preferences.
- Check the stop button. It will prompt for your password enter the administrator name and password and click ok.
- To customize this service if it is going to be run click on the Open Sharing Preferences button in the Back to My Mac tab of the Mobile Me System Preferences.
- Choose the specific services you would like to share such as file sharing or screen sharing.

Network

The Network pane contains per-interface network settings. In general, disable unused interfaces. Wireless networking shouldn't be used for servers unless absolutely required. Here are some recommendations for any network interface:

- When possible, configure IPv4 addresses manually, rather than using DHCP.
- Disable IPv6 if it isn't used.
- Leave Make AppleTalk Active unchecked.

Note: When possible use a proxy for Internet connections. This improves performance and security of these connections.

Wireless Networking

To secure the wireless networking:

- Open System Preferences.
- Select Network Preferences.
- Select Airport.

- Set By default, 'Ask to join to new networks'
- Then press the 'Advanced…' button and configure the following:
  a) Check "Require Administrator password to control airport"
  b) Consider un-checking 'Remember any network this computer has joined'
  c) Consider checking 'Disconnect from wireless networks when logging out'
- Make sure that when connecting to wireless networks that you never use WEP. Always use WPA or WPA2 if at all possible.

Due to attacks like those released at BlackHat by David Maynor and Johnny Cache, disable Airport when wireless is not required. To do so:

- Click on the Airport icon at the top of the screen.
- Select the 'Turn Airport Off' menu item.

RADIUS is required to use the WPA2 Enterprise feature of the Apple Airport. 10.5 has no built-in RADIUS server: MacRADIUS is available at http://www.macradius.com.

Bluetooth

If your device has Bluetooth support, go the Network pane, and click on Bluetooth. Choose 'Set Up Bluetooth Device…'

- Uncheck On.

If you must enable it, make the system less likely to be found by:

- Uncheck Discoverable.

Unless you need to be able to wake the computer with a Bluetooth device (say, a cordless keyboard or mouse),

- Uncheck Allow Bluetooth devices to wake this computer.
- On the Sharing tab, disable all unused services.

One danger behind the use of Bluetooth is Bluetooth file sharing. To secure the Bluetooth File Sharing features:

- Go to the Sharing tab of the Bluetooth System Preference.
- Uncheck items that you will not be using to share data with Bluetooth.
- Check the password option for all items that are enabled.
- For Bluetooth File Transfer:
  a) Select the folder with files that should be shared. Make sure only items that are required to have remote access are located in this folder.
  b) Check the box for Require pairing for security.
- For Bluetooth File Exchange:
  a) Select the appropriate folder.
  b) Check the box for Require pairing for security.
- For Bluetooth-PDA-Sync:
  a) Select the type of Serial Port interface for Bluetooth to mimic.
  b) Check the box for Require pairing for security.
  c) Check the box for Show in Network Preferences.

QuickTime

To avoid potential malicious content downloaded from the web, a situation that has happened in the past:

- Uncheck Play movies automatically on the Browser tab.

Sharing

Reducing the number of services in reduces the attack surface of your system:

- Disable all unused services on the Services tab.

If you enable Apple Remote Desktop(Remote Management):

- Click the Access Privileges button and configure the following:
- For each user, only grant those privileges that the user requires under Allow user to do the following on this computer.
- Uncheck Guests may request permission to control screen.
- Disable VNC connections if possible; otherwise, require a strong password.

On the Internet tab, leave Internet Sharing off unless you need to share your network connection with other computers. If you use AirPort to share your connection, be sure to follow the recommendations on Wireless Networking elsewhere in this document.

The ipfw.conf file and the ipfw command line utility, located at /etc/ipfilter/ipfw.conf, can be used to customize firewall rules beyond what is available in the GUI. In addition to ipfw there is dummynet, which can be used to shape traffic and impose bandwidth limits using a variety of parameters. The security section of this document outlines additional firewall options and should be reviewed as needed.

Accounts

System administrators should have unprivileged accounts for performing many of their daily tasks and a separate administrative account for system maintenance only. In most cases, a sysadmin will automatically be prompted for administrator credentials when performing administrative actions as an unprivileged user. For more intensive administrative tasks, the sysadmin can use Fast User Switching to login to the special administrator account.
To make an account unprivileged:

- Uncheck Allow user to administer this computer on the Password pane of the Accounts section in the System Preferences application.

Each sysadmin's administrative account should have an inconspicuous user name (not *Administrator*), a strong passphrase. Once these settings have been set:

- Allow user to administer this computer checked.

On the **Login Options** tab:

- Uncheck Automatically log in as.
- Set Display login window as to Name and password so as not to give an attacker a list of valid usernames.

- Uncheck Show the Restart, Sleep, and Shut Down buttons to prevent denial of service.
- Uncheck Show password hints to avoid displaying user-chosen hints that could be too revealing.
- Fast user switching should only be used on computers where the user community is trusted. Rouge process can stay resident in the background even if another user is using the computer.

Date & Time

An accurate clock can be important for network file systems and authentication services such as Kerberos. To set a network time server:

- Check Set date & time automatically to synchronize your clock with one of Apple's time servers.
- If possible, you should change this server to a locally maintained one.

Software Update

- Set the Check for Updates option to Daily.

To enable the system to remind users of pending updates no more than a day after they become available:

- Check Download important updates in the background.

Apple has separated security updates from software updates. Most security updates will not require a restart. These should be applied those updates as soon as possible, even if you're not connected to a network.

If running as an unprivileged user, as recommended in the Accounts section, Software Update will not run automatically for you. For this reason, you should follow a regular schedule including:

- Manually checking for updates or use a third-party program or script to do it for you.

Speech

Text-to-speech and speech recognition can result in data leakage or unauthorized access. To prevent an attacker from verbally controlling your computer:

- Leave Speakable Items off on the Speech Recognition page.

If Speakable Items must be used:

- Select Listen only while key is pressed.

To prevent information leakage:

- leave Announce when alerts are displayed.
- Leave Announce when an application requires your attention unchecked.

Universal Access

To deny access to additional scripting capabilities which could otherwise be abused by malware:

- Uncheck Enable access for assistive devices.

You can also prevent audible data leakage by:

- Disabling VoiceOver on the Seeing pane.

Locking and Unlocking System Preferences

Once you've configured everything within System Preferences, you should lock the System Preferences to prevent changes.

To lock System Preferences:

- Choose one of the specific preferences sections like Security.
- If the padlock icon at the lower left of the window looks unlocked, click it to close the lock.

To unlock System Preferences:

- Choose one of the specific preferences sections like Security.
- If the padlock icon at the lower left of the window looks locked, click it to open the lock.
- Provide System Administrator credentials to unlock the preferences.

Note: In several different places in this checklist, you are asked to make changes within System Preferences. If the System Preferences are locked, many of the choices will either be grayed out, or may simply look different. It is also important to require a password to unlock each of the System Preferences. This is covered under the security section of this document.

Securing the System and the Data

Open Firmware and EFI Password

Open Firmware, developed by Sun Microsystems, is the technology that Apple used for its PowerPC platforms. Extended Firmware Interface or Extensible Firmware Interface (EFI) is Intel's vision for the replacement of the Basic Input/Output System (BIOS) that has been a PC and compatible standard for decades. Apple has architected their Intel platform with EFI rather than the traditional Open Firmware. So, this section is broken into Open Firmware and EFI, because they are different and setting a password in them is slightly different as well.

Setting an open firmware password will prevent people from forcing your Mac to boot from other modes than to the hard drive. This includes booting to Firewire drives, firewire target disk mode or CD/DVD optical drives. You should set this password to something that you will remember but if you forget the password it is always possible to alter your RAM configuration and reboot to reset the password. If you have access to the system then it is also possible to decipher this password as it is stored in a simple hexadecimal encoding. Due to this it is a good idea to use a password that is not used for non-physical security management in your environment.

To enable the Open Firmware password setting and set the Open Firmware password on OS X on a Power PC (PPC) machine, the following steps should be followed:

- Restart your computer while holding down the Command, Option, O and F keys.
- This will then load up the Open Firmware.
- At the Open Firmware prompt type the following: >password
- Then type in the password that you want to set, once you have entered the password you will be prompted to enter the same password again, this is done to make sure that you entered the password correctly.

This password can be up to eight characters in length, and you must not use the capital letter "U" in your password as this can cause problems (http://docs.info.apple.com/article.html?artnum=107666). Once the password is set you can enable the password feature. At the prompt then type the following to stop booting from any other devices without using the password that you specified:

- >setenv security-mode command

The final step is to then type the following at the prompt to restart the computer:

- > reset-all

For Intel Macs, setting an EFI password is similar. First, the steps above have you enable the features from within Open Firmware itself, prior to system boot. EFI has no features, at least that Apple has documented, so to manipulate the firmware password on Intel Mac computers, you install the Open Firmware Password Application. For versions of OS X prior to 10.4, you can download it from Apple's web site. OS X 10.4 and beyond requires a newer version of the password application, and for some reason, Apple only provides it on the Software Installation Disc. Starting with OS X 10.5 the OS X installation disk must be used as the boot device to set the firmware password. The name of the application was changed to Firmware Password Utility:

- Insert your OS X installation CD.
- Reboot your computer.
- Boot from the CD/DVD hold the letter C to accomplish this.
- When the installation program comes up choose utilities out of the menu bar.
- Select Firmware Password Utility.
- Check the Require password to change firmware settings checkbox.
- Type in the password in both the password and verify password fields.
- Click OK.
- Quit the Firmware Password Utility.
- Reboot the computer and remove the installation disk

Note: When using a MacBook you should run the MacBook SMC Firmware Update on Apple's site before make any firmware changes.

File Permissions

Thanks to OS X's UNIX core, file permissions on OS X are very similar to other flavors of UNIX. There are the standard POSIX compliant owner permissions, owning group permissions, and other or world permissions, with permissions being read, write, and/or execute. How the meaning of these read, write, and execute permissions differ between files and directories is also the same as other flavors of UNIX. Again, like other UNIX flavors, OS X understands the umask concept as well. A detailed explanation of these capabilities is beyond the scope of this document.

This section isn't so much about file permissions, as it is about how to set up your system so that files are created with secure permissions, and how to find files with potentially weak permissions. We'll talk more about securing existing file permissions further down.

Change the default umask

The umask is short for user file-creation mask. Like file permissions in octal format, the umask is an octal number. File and directory permissions are technically a 4 digit octal number, but the left most digit is optional unless you're specifically trying to set that set of bits. For some reason in at least some versions of OS X, the umask displays as a 4 digit number with a leading 0, but technically, you can't change that digit; only the last 3 digits. Each digit of the umask is subtracted from 7 to give you the permissions for a newly created file. For example, if the umask is 0022, then a newly created file would have permissions 755, or user=read,write,execute, group=read,execute,other=read,execute.

In OS X the default umask is 022. This means that everyone will have read permissions to all newly created files. It's a good idea to change this umask to 027, which removes all access to “everyone”. What isn’t standard UNIX in this case is OS X using base 10, instead of base 8. Octal 027 == decimal 23. So, in a terminal window, or from a script type the following:

```
sudo defaults write /Library/Preferences/.GlobalPreferencesNSUmask 23
```

NOTE: there is a file called /Library/Preferences/.GlobalPreferences.plist, but that is not what we want to type in the command. We want the GlobalPreferences domain. Shell expansion, might add the “.plist” part: be careful. You’ll need to logout and back in, as this setting takes affect at login time.

Find weak file permissions

So, now we’ve taken care of files that will be created in the future, but what about files already created? We need to find all the files that have weak permissions. To find files that have world write permissions:

```
sudo find / –perm –002
```

This will produce a list of files that are world writable. Another problem is looking for programs that are Set User ID (suid) and world executable. suid and Set Group ID (sgid) deal with that 4th octet I was speaking about above in the umask section. When this is set, the execution of the program is run with the program owner’s or program group owner’s authority, not the authority of the user who executed the script. A classic example is the su command. This command will let you switch to another user in a terminal window. This program is owned by root, and needs to be run with root authority, so that it can switch you to the other user (possibly root itself). Everyone has execute permissions (both group and other) because everyone has the ability to switch to another user if they know that user’s password.

It’s possible, however, that there are programs that don’t really need to be suid or sgid. To find these ID’s:

```
sudo find / –perm –4000 –o –perm –2000 [–a –user root ]
```

The [-a -user root] is optional. Sometimes you might only be concerned if a program is SUID/SGID if the privileges granted would be for root. Consult your man page for the find command to extend the complexity of the search. Be very careful changing file permissions that are suid or sgid, because if you remove that permission you could break the system. Generally, we’re looking for them to remove the world execute privileges, not the suid/sgid privileges. The best way to stay out of trouble is to perform this find on a brand new system, and assume that (for the most part anyway) those permissions are correct. Then you just run this again periodically and compare the results to the original run. Just add a:

```
><filename>
```

… to the end of the find command and the output will go to that file, instead of standard out.

File ACLs

As a lot of other flavors of UNIX are implementing file ACLs, as of 10.4 OS X has extended file ACLs as well. Theses ACLs provide for more granularity beyond traditional UNIX file and directory permissions. Again, a detailed explanation of these capabilities is beyond the scope of this document.

First, you have to enable file ACLs. By default, they are disabled in OS X 10.4. To enable them:

```
sudo /usr/sbin/fsaclctl -p / -e
```

To enable a user based ACL for a file called secrets.txt:

```
chmod +a “joeuser allow read” secrets.txt
```

To enable a group based ACL for the same file:

```
chmod +a “administrators allow write” secrets.txt
```

With ACLs you can also specifically deny access. So, we've allowed the administrators to have write access, but what if we don't want user bob to have write access. Let's deny bob access:

```
chmod +a “bob deny write” secrets.txt
```

To view ACLs from the command line:

```
system $ ls -le secrets.txt
-rw-r----- + 1 user1user1  0 Oct 12 10:27 secrets.txt
 0: user:joeuser allow read
 1: group:administrators allow write
 2: user:bob deny write
system $
```

Encrypting Home Folders

On OS X it is possible to have all the files and folders within your home directory encrypted on the fly using AES-128 bit encryption. This is done using the FileVault (see the System Preferences section). It is a good idea to enable this on all portable computers. One thing to remember here though is that if you have a large iTunes library, it is a good idea to move it out of your home directory as this can cause problems.

First, from the/an administrator’s account:

- Create the FileVault master keychain
- open System Preferences->Security.
- Click on the FileVault tab
- Click on the Master Password item and then set a master password.

Select a strong password here, and do not use the same password that you use to login in to the system with.

Then, within each account that you want to have an encrypted home directory:

- Open the Security System Preference.
- Click the “Turn on FileVault” button.
- Check Use secure erase so that files will be overwritten with patterns when deleted so their contents cannot easily be recovered by an intruder.

This will then log you out of your system and then encrypt your home folder. This can take a while, so be patient here. Once done, your system will reboot, and your home folder icon should now look like a safe.

Recently whole disk encryption has been released as an addon to Mac OS X. Both Checkpoint and PGP offer competitive products that encrypt the entire contents of both the Mac boot volume as well as external drives.

Keychain Services

A keychain is like an encrypted vault for storing sensitive information. Each user gets a Login keychain when their account is created, but they can have as many keychains as they like.

The Login keychain's password defaults to their system password, but there is no need for it to remain that way. If the user's system password is the same as their keychain password, and the keychain is set to be unlocked while the user is logged on, then the user won't be prompted for the keychain password when the Login keychain is unlocked. If the passwords aren't synchronized, then the users will be prompted for the Login Keychain password separately. It's a security versus convenience trade off that each user and/or organization will have to make.

The keychain has two levels of access. Unlocking the keychain allows the user to view “titles” of entries in the keychain, but not the secure part of the entry. For a password item, all the information about a password item like the user name etc. is viewable when the keychain is unlocked, but the password is not.

The user has to click the “show password check box” to see the password, and will be prompted for how long they wish to be able to view the password: Deny, allow once, Allow always. If “Allow Once” is checked, it's only allowed until the either the user unchecks the “show” box or closes the keychain.

Under “Edit | Change settings for Keychain <chain name>, some of these defaults can be changed. To secure each keychain:

- Open the Keychain Access utility from /Applications/Utilities/Keychain Access
- Click on the Keychain you would like to secure.
- Click on the Edit menu and Select Change Settings for Keychain
- Check the box for Lock after x number of minutes

- Fill in the inactive period
- Check the box for Lock when sleeping
- Click Save

If you are using a trivial password for the keychain consider using a strong password. To reset the keychain password:

- Open the Keychain Access utility from /Applications/Utilities/Keychain Access
- Click on the Keychain you would like to secure.
- Click on the Edit menu and Select Change Password for Keychain
- Enter a new password for the Keychain.

Passwords for web sites and SSL certificates are also stored in Keychain access. If a website has its SSL certificate revoked due to time or improper use of the site it will appear in the revocation list. X509 Anchors is a location where you can view SSL certificates. To remove sites that have had their SSL certificate revoked:

- Click on the X509 Anchors item in the Keychains portion of Keychain Access.
- Click on the site (it will be indicated with a red “X”).
- Click on the Edit menu.
- Select Delete.

System Integrity

While most of this checklist deals with preventative measures, this section is dealing with system validation and auditing. It is preferable to prevent a security violation from occurring. However it is not realistic to consider you will always be able to prevent intrusions and may need to detect that an event has occurred and isolate the effects it has had.

NOTE: Some auditing and logging tools use large amounts of disk space, which should be considered when using them.

NOTE: The information from many tools can be compromised by an administrative account. Multiple administrative accounts can often reduce the likelihood of a clean audit trail.

Auditing and Logs

A key to securing a system is to review what is happening on the system on a regular basis. This is true whether an intrusion is suspected or not. To properly review events on a system and isolate what may have occurred use both the logging tools and auditing tools that are provided by Apple.

Logging is the recording of various communication events between different systems within a computer. Some of these events are security related, while others are just helpful to determine why an error is occurring as is common with troubleshooting. The Console application is used to view and maintain log files on the system. The Console application is located in the /Applications/Utilities/ folder.

Console gives one application where different types of events can be viewed. These include any logs stored in ~/Library/Logs, /Library/Logs and /var/log. The ~/Library/Logs folder contains user-specific logs, such as a user's activities within the Disk Utility Application, the optical burning capacities of the system and many third party applications such as Java. The /Library/Logs folder contains many third party application logs that do not deal with user specific issues. Some of the logs in /Library/Logs also deal with Apple-specific items that are shared amongst other items and the logs pertaining to some of the file sharing services such as SMB. The /var/log is where the bulk of security-oriented logs are stored, including logs for the firewall, ftp, printing, virus scanning (for the mail server in OS X Server) and the web server.

The BSD subsystem handles most of the important system logging, while some applications choose to handle their own logging. Like other flavors of Unix, OS X uses the syslogd daemon to facilitate system logging, and its configuration file is /etc/syslog.conf. Syslog.conf can be edited using the Terminal. The default entries in this file are sufficient, but you may wish to tweak them for your own needs if you are having a security issue or require more information as is often the case with debugging.

Each line in the syslog.conf file contains a facility, a priority and an action. Facilities are categories of messages like mail and kern (kernel). Priorities denote the urgency of the message from the least important to the most critical. Priorities include debug, info, notice, warning, error, crit, alert, and emerg. The priority can be set by applications rather than syslogd. The action setting controls what occurs with the message for a particular facility and priority. Here's an example entry that can be used to control mail logs:

```
mail.emerg          /var/log/mail.log
```

The above line causes log messages of the mail facility with a priority of emerg or higher to be recorded in the /var/log/mail.log file. Emerg is the highest priority; if a priority of alert had been used in the example, mail.log would receive messages with the priority of alert and emerg.

Syslogd only logs items to the local system; however the syslogd daemon has the capability to log this information remotely. With sensitive systems, consider doing this, as a user with enough system privileges can easily change the contents of the log files. Asample configuration line in syslog.conf for a remote log:

```
Mail.emerge         @your.servername.here
```

You would replace “your.servername.here” with the name of your remote log server. By the way, changes to the syslog.conf file, don't take effect until you restart or “HUP” the syslogd daemon:

```
Sudokillall –HUP syslogd
```

Many logs can take up a large amount of disk space and even longer to review. If you’re capturing this information, then it should be reviewed. If you would like to use your computer rather than spend all of your time administrating it there are some tools available that assist in analyzing the information more efficiently. Swatch, Sawmill and logsurfer are tools that can require extensive setup prerequisites and configuration, which goes beyond the level of detail we’re capturing in this checklist. Swatch can be found at http://swatch.sourceforge.net/ and logsurfer can be found at http://logsurfer.darwinports.com/. Sawmill is available at http://www.sawmill.net.

As with most Apache distributions there are a variety of tools available to analyze the web logs specifically. Most of these are geared towards determining traffic flow on the website but some can help with security. Web analytic packages include AWstats, Webalizer, Peastat.and any others that can be run on Apache.

Host Based Intrusion Detection

A Host Based Intrusion Detection System (HIDS) can mean different things to different people. Some consider a HIDS to mean a file hashing system such as tripwire; others consider HIDS to denote a daemon detecting unusual or unauthorized events running on the system. When it comes to the term HIDS, both types can be referenced as HIDS. We'll be discussing the local daemon type here, and covering the file hashing type below.

Most HIDS that can currently be run on OS X fall in the File checksum category.
OSSSEC http://www.ossec.net

- PortSentrySentry Tools: http://sourceforge.net/projects/sentrytools/
- Little Snitchhttp://www.obdev.at/products/littlesnitch/index.html

File Checksum generation and Comparison

While it is possible to create your own file integrity system with OS X, it comes with OpenSSL installed by default. Using the OpenSSL command to run a checksum of individual files is one way of establishing a file integrity system. A shell script can then be used to compare checksums of known good versions of the file with the current checksums and either log changes into syslog or alert an administrator of changes to the filesystem. An example of using this includes:

```
$ openssl MD5 <file>
MD5(<file>)= c71ef93bdd7f73b468b8a0615e2a585b
```

Most organizations will want a polished product when managing multiple systems. One solution to accomplish this is to use Tripwire. The open source version of tripwire is available at the following locations:
http://sourceforge.net/projects/tripwire
http://www.macguru.net/~frodo/Tripwire-osx.html
http://www.frenchfries.net/paul/tripwire/index.html

Checkmate is a GUI utility that can be used to run checksums of existing files and compare them to future checksums. Tripwire installs a new preference pane into the System Preferences of systems and provides an easy-to-use interface to allow snapshots of important files on critical systems Tripwire is available at http://personalpages.tds.net/~brian_hill/checkmate.html

Network Intrusion Detection

A Network Intrusion Detection System (NIDS) reads patterns of network traffic and typically looks for patterns known to represent attacks on the system. The most common Network Intrusion Detection System in use on a Mac is Snort. Snort is available at http://www.snort.org/ and a good HOW-TO for it can be found at http://homepage.mac.com/duling/halfdozen/Snort-Howto.html.

Bastille

Bastille Linux is a hardening suite for Unix-like operating systems. Bastille automates many of the steps recommended by this guide, and is an excellent choice for hardening any supported OS.

Support for Bastille for OS X has now reached 'stable' status. It may be downloaded here: http://www.bastille-unix.org/running_bastille_on.htm

HenWen is a GUI application available for Mac OS X that can be used to control Snort. This puts advanced network signature scanning capabilies without the need to have in depth knowledge of what is being scanned. HenWen comes with a script that will automatically update the firewall configuration to block IP addresses suspected of violating Snort rules. This turns HenWen into a Network Intrusion Prevention System. HenWen is available at http://seiryu.home.comcast.net/henwen.html

There are many that will tell you that Antivirus software is not required for OS X, for various reasons like "it's secure" or "viruses don't work on a Mac". Many will point out that there are no known viruses for Mac OS X. However, this is not true for Trojans. There are many documented Trojans available for the Mac. While OS X has a secure design, and there is less malware for OS X, not having Antivirus software is never a good idea.

As Mac OS X gains in popularity, it continues to become a larger target for malware authors. Products like Microsoft Office are available on the Mac platform, and some Office macro viruses work on OS X and can infect the Normal template as is the case in Windows environments. For viruses and Trojans that cannot infect the Mac, they may be responsible for sharing these threats to users of other platforms by receiving and passing on documents and binaries.

There are several commercial Antivirus products for the OS X platform: McAfee's Virex, Symantec's Norton AntiVirus, Sopho'sAntiVirus, and Intego'sVirusBarrier. There is also an Open Source antivirus product, ClamAV. ClamXav is a GUI tool that can be used to run ClamAV. ClamXav is lacking in many basic features like having a resident daemon to scan files as they're manipulated, it does a find and quarantine infected files. The use of ClamXav should be restricted to environments where it is used as an early warning sign of infections.

ClamXav is available at http://www.clamxav.com. Norton Antivirus is available at http://www.symantec.com. Many organizations already have an enterprise package for virus scanning. Sophos, Intego and McAfee can all be used in conjunction with their corporate/Enterprise counterparts. This allows for a centralized administration console. Norton Antivirus also has this capability, but only when used in a "command-line only" mode.

Note: At this time Norton AntiVirus is the only product available that is capable of cleaning infected files. Other products will simply quarantine infected files. In many outbreaks there will be hundreds of infected files, representing a large quantity of data to have quarantined

Mac OS X Server Specific Security Checklist

OS X has a built-in firewall for limiting access to network services. This can be used to limit access to server resources based on subnets. You can also reduce your server's attack surface even further by running as few services as possible. Simple configuration of services is done using the *Server Admin* tool (located in the /Applications/Server folder).

Before you begin configuring a specific service for a more secure setup (or make any alterations to it for that matter) you should backup the settings for the service. To do this:

- ▫ Click on the settings icon in the lower right hand corner of the screen for the service.Open Terminal.
- ▫ Drag that icon to your desktop.Run the following command, substituting afp with the name of the service you would like to backup settings for and substituting ~/afpsettings.txt with the actual path and filename for the file you would like to backup your settings to.

sudo serveradmin settings afp > ~/afpsettings.txt

- ▫ Open it to make sure it contains the service settings you will be changing.View the file and verify all settings backed up as needed.

Services Access

The following blanket recommendation applies to any network service, including those not listed here:

- ▫ Disable any network service that is not used.

Follow the checklists below for any services that must be enabled. If a service is enabled and there are no user access controls then it is possible to control many of the services by clicking on the servers name under the SERVERS list, clicking on the Settings icon in the toolbar and then clicking on the Access tab. Here you can configure Service Access Control Lists (SACLs) by using the Allow Only Users and Groups Below: to specify which users can access each service, by service. Services with SACLs include AFP, Blog, FTP, iCal, iChat, Login Window (similar to the log on locally option in Windows), Mail, Podcast Producer, QuickTime Streaming, RADIUS, SMB, SSH, VPN and Xgrid.

Additionally, you can granularly configure which users have access to administer or monitor each service using the Server Admin tools. This allows you to have a layered approach to administer the server services. To do so:

- ▫ Open Server Admin and click on the name of the server in the SERVERS list that you would like to configure administrative access to.
- ▫ Click on Settings in the Toolbar.
- ▫ Click on the Access tab.
- ▫ Click on the Administrators sub-tab.
- ▫ Click on the For Services Selected Below radio button.
- ▫ Click on the Service for which you would like to configure.
- ▫ Click on the + icon below the list.

- Drag the user or group to allow administration for (or specifically restrict administration for.
- Select Administer or Monitor in the list to determine what level of access a user has

Network Services

The *SERVERS* pane on the left side of the *Server Admin* window contains an expandable list of computers with their installed network services. The remainder of the window is dedicated to information and configurable options for the selected computer or service. Items in the toolbar along the top of the screen allow you to get an *Overview* of the service, view *Logs*, list *Connections*, view *Graphs* of usage statistics, or configure service-specific *Settings*. Some services may not have all of these items in the toolbar, or may have other service-specific items, such as . The actions on the checklists below are made by selecting the Settings icon in the toolbar and then selecting one of the upper tabs as indicated.

There's not room in this document to review all of the possible settings for every service, but we call attention to security-specific steps you can take. If you are running a service, then you should review the documentation for how to secure that service by the open source project for which the service is based (eg – Apache documentation for the web service or Samba documentation for the Windows service).

AFP

The Apple File Protocol (AFP) service allows clients to mount shared folders from the server. By default, file servers advertise themselves using Bonjour and AppleTalk to appear in the Finder on every other computer on the same network. The number of users accessing AFP is unlimited by default, no logging is performed, and idle users remain connected indefinitely.

These default settings are not as secure as they should be.

- On the General tab, consider disabling Bonjour registration if you will be using IP or DNS for users to access the server.
- On the Access tab, use Kerberos authentication if possible. Disable Guest access and the option to Enable administrator to masquerade as any registered user, which allows administrators to authenticate into any user account using any administrator password. Limit Client and Guest connections to a small but reasonable number for your service, say 100 or 500 according to the size of your deployment.
- Enable the access and error logs on the Logging tab.
- On the Idle Users tab, consider disconnecting idle users after 10 minutes, and uncheck all the exceptions when possible.

Note: It is also important to consider the fact that AFP does not log the paths of files accessed, only relative paths on file access. This makes file auditing difficult for directories and does not provide an administrator or forensic investigator with a very comprehensive audit trail of access. One item that helps here is that the AFP service does log access to "." files which can help enumerate the actions of users as they traverse the shared portion of your file system and logs the IP address and user name used to login. Therefore you can triangulate who logged in and what they accessed unless you are using the Enable administrator to masquerade as any registered user.

DNS

The DNS service allows other computers to use your server to look up hostnames.

- On DNS servers, limit zone transfers and limit recursion to hosts needing each under the Settings icon in the toolbar.

Firewall

OS X Server offers a more robust graphical interface for maintaining the firewall than client versions of OS X. As always, customizing the *ipfw.conf* file is available for more granular access control than what is available in the graphical interface. To configure your settings, click on Settings in the toolbar.

- On the Address Groups tab, configure all the address groups you will use rather than hard-coding addresses into your ruleset. This technique will help keep your ruleset to be more easily maintainable.
- On the Services tab, you can specify which protocols you want to allow for each of your address groups. You can also add your own services.
- Using the Logging tab you can specify which type of events to be logged, as well as the maximum size of the ipfw log.
- On the Advanced tab, you can add rules almost exactly as they would appear in the ipfw ruleset. You can also use the Advanced tab to enable Stealth Mode for UDP, TCP or both.

Here are some suggestions on building a firewall ruleset:

- Use a default-deny policy. That is, only allow that which you absolutely need.
- Apply policies in both directions. For example, block incoming TCP port 25 if you're not running a public mail server, but also block outgoing TCP port 25 if the server doesn't need to send mail.
- When applying a ruleset to an existing server, test it first. Add a logging rule that allows all traffic at the end of your ruleset but before any default-deny rule. For example, on the Advanced tab, click the + button to add a rule. Set **Action** to **Allow.** Set **Protocol** to **Other**… and type all. Set **Service** to **Other**…. Check **Log all packets matching this rule**. Set source and destination addresses to **Other**… and type any. Set **Interface** to **Other**… and type any. When you enable the firewall, all your services should continue to work, but you'll get a log of all the packets your rulesetwould have blocked if it weren't for your logging default-allow rule. You can remove that rule once you're sure of your ruleset.

Note: Dummynet can be used to throttle bandwidth for specified rules. This addition to ipfw can be a good method of mitigating the use of Denial of Service attacks against services running on your server.

FTP

In Leopard, FTP is a Kerberized service in Mac OS X or Mac OS X Server.:

- Using the General tab, set the Authentication tab to Kerberos authentication. Do not

enable anonymous access. Additionally, set a maximum number of authenticated users here.
- Using the Advanced tab, set Authenticated Users See in such a way that users see only data they need to access. You can use the NFSHomeDirectory attribute for a user account to manually configure the specific folder a given user can access when you have users able to "see" Home Directory Only.
- On the Logging tab, check all the boxes to enable complete logging.

Even with the addition of Kerberos, FTP is not terribly secure. When possible, use WebDAV or another alternative . If you need to use FTP then consider an alternative to the default FTP server in Mac OS X such as Wu-FTP or Rumpus, a popular FTP application which jails all users by default or implement FTP jails.

iCal
The iCal service is new in Mac OS X 10.5. iCal relies on CalDAV to provide calendars to client systems. To secure the iCal Server, open Server Admin and click on iCal for the server you are securing and then click on the Settings icon:
- Limit Attachment Size to accommodate your workflow.
- Enable User Quotas when appropriate.
- Set the Authentication to Kerberos when available.
- Enable SSL and use a good certificate.

Additionally, in Workgroup Manager, you should only enable iCal for users that need it.

iChat
The iChat service is based on the open source jabber package. iChat Server is used to allow users to chat with one another using jabber compliant software.
- Set the Authentication to Kerberos when available.
- Choose an SSL certificate.
- Disable Server to Server Federation unless it's being used for your environment.

Mail
The Mail service provides network mailbox storage (POP and IMAP) and mail transport (SMTP). Mail can be further secured by the use of the following:
- On the General tab, disable any of the services (POP, IMAP, and SMTP) that are not used. If the server is only meant to send mail, uncheck **Allow incoming mail**.
- On the Relay tab, restrict the hosts and networks that are allowed to relay and configure any Realtime Blacklist Servers (RBLs) if your organization uses them.
- On the Filters tab, enable the scanning of mail for viruses and daily updates of the virus database. Also, consider enabling scanning for spam, which is performed by spamassasin.
- Using the Quotas tab restrict the size of incoming messages.
- On the Mailing Lists tab, leave mailing lists disabled if they are unused.
- Configure cryptographically secure authentication methods (Kerberos or CRAM-MD5) using the Advanced tab. Disable Clear authentication. Require SSL for SMTP, IMAP, and POP if possible.

Note: When restricting access for hosts allowed to relay through an OS X mail server make sure not to allow the firewall to relay or you could be opening all systems outside of your environment.

MySQL
Prior to Mac OS X 10.5 MySQL was administered in a stand-alone application. In 10.5, MySQL has been moved into Server Admin. Many of the security-centric aspects of MySQL should be managed in the my.cnf file or using MySQL tools. However, there are a couple of things you can do to further secure your database deployment using Server Admin.

- Disable network connections unless the database actually needs to be accessed from hosts other than the server.

NetBoot
NetBoot allows Mac-based devices to boot using system software off a network share.On the Filters tab, check **Enable NetBoot/DHCP filtering** and provide a list of allowed clients.

- Set the **Log Detail Level** to **High** on the Logging tab.

Note: NetBoot uses the TFTP protocol by default. TFTP is a very weak protocol from a security perspective.

NFS
NFS is a file-sharing protocol. Classically, it provides no cryptographic authentication or encryption and authenticates users based on IP addresses rather than a username and password. This makes it susceptible to a variety of attacks. However, in Mac OS X 10.5 NFS is secured using Kerberos. However, in most cases you may still choose to disable NFS.

- Disable NFS.

But if you must use NFS then consider deploying one of the following options for each sharepoint in Workgroup Manager:

- Map Root User to Nobody

Open Directory
Open Directory allows a Mac OS X computer to receive information about users accounts and policies from a master server. This is similar to other directory services in other operating systems such as Microsoft's Active Directory. If policies will be used to control various aspects of the desktop interface then Open Directory will be needed.

Open Directory maintains the Kerberos KDC (Key Distribution Center) for Open Directory environments. By moving into a Kerberized environment it is possible to reduce the passwords being sent over the network. This allows for more secure communication and only one password to be used in an environment. When operating in a Kerberized environment, it is possible to use many different services, such as email, websites, AFP and QuickTime after only entering the one password required to login to the environment.

Another advantage to Open Directory is the strong password policies that can be deployed when using Open Directory. This includes requiring strong passwords and password lockout policies.

To further secure Open Directory beyond the default configuration:

- On an Open Directory server, limit the number of results that can be returned via LDAP on the Protocols tab. Also, enable Secure Sockets Layer (SSL) for LDAP, selecting a secure SSL certificate.
- On the Policy tab, configure the Passwords sub-tab to match your site policy.
- On the Bindings sub-tab of the Policy tab, check all the options under Security when possible.
- On the Security sub-tab of the Policy tab, disable LAN Manager hashes and any other hashes you don't use. Under **Recoverable Authentication Methods**, disable all the methods you don't need.
- Using the slapd.conf file, impose stringent Access Control Lists using standard LDAP ACL configurations.

QuickTime Streaming

Using QuickTime Streaming Server (QTSS) it is possible to host QuickTime content and stream it to clients. QTSS can also accept incoming MP3 broadcasts, broadcasts from QuickTime Broadcaster and perform many other functions. Some of these functions open additional network ports and should be disabled if unused. To do so:

- On the General tab, set **Maximum connections** and **Maximum throughput** to appropriate values based on the abilities of your server and network connection.
- On the Access tab, set a strong **MP3 Broadcast Password**. Unless you use them, disable **incoming broadcasts** and **home directory streaming**, and leave **Enable web-based administration** unchecked. If you choose to enable incoming broadcasts or web-based administration, set strong passphrases for each.
- Leave both the error log and access log enabled on the Logging tab.

RADIUS

RADIUS (Remote Authentication Dial In User Service) is a protocol that can be used to control access to network resources. When you are using VPN or WPA2 Enterprise for your wireless environment, RADIUS should be enabled to further secure them. Additionally, RADIUS can be leveraged to provide secure sign on for other, third party services such as the CommuniGate Pro Mail Server.

VPN

The VPN service allows you to create a secure tunnel endpoint on your server. PPTP is the most common type of VPN made available in OS X Server environments. When possible it is a good idea to restrict VPN access to L2TP clients as they use a more secure tunneling method. To do so:

- If possible, enable L2TP with Kerberos authentication, and disable PPTP.
- When using L2TP, prefer certificate authentication over shared secret or use RADIUS

authentication with PPP.
- Use the Client Information tab to restrict what client systems have access to.
- On the Logging tab, leave **Verbose logging** enabled.

Web

OS X Server comes with an Apache-based web server built in. As with any web server, it's vital to enable it only if you need it and configure it with security in mind. Due to the feature rich nature of Apache it is vulnerable to a variety of attacks ranging from cross-site scripting attacks to getting turned into a phishing server. To secure the default Apache server using Server Admin:

- Configure the General tab using values appropriate for the capabilities of your server and network connection. Apache's Performance Notes page (http://httpd.apache.org/docs/1.3/misc/perf-tuning.html) gives some advice on setting these values.
- Under the MIME Types tab disable any file types unused in your environment.
- Using the Proxy tab, configure a proxy to sit between the web server and client systems when possible.
- On the Modules tab, disable all modules that aren't used. For maximum security, start with all modules disabled, then enable them one by one until your web site starts working again or research which are required and disable those that are not.
- Click on the Web Services tab and set an attachment maximum.
- Under the Sites icon in the toolbar, select each site in turn and click the edit button below (it has a pencil icon). Using the Security tab enable SSL for all sites where SSL is appropriate. On the Options tab, disable every option that isn't needed. On the Security tab, enable SSL unless there is no consequence to an attacker eavesdropping on or modifying web transactions in either direction. Using the Realms tab, set a password for sites that should be password protected. Using the Web Services tab, disable, webmail, wiki, web calendar, mailing list web archive and blog unless you are using these.

Many of the Apache modules that you might use will have their own specific security concerns. Read up on the developers site for each module used in order to maximize the security of these modules.

Note: In Mac OS X Server 10.4, Server Admin had a service item specifically for Application Server services. These items have been moved to

SMB (formerly Windows)

The Windows service in Mac OS X and Mac OS X Server has been renamed to SMB in 10.5 to accurately reflect the open source software for which it is based. SMB uses Samba as the back-end engine to provide file sharing services to Windows clients. Mac OS X Server can be a member of a Windows domain using SMB to allow administrators to further leverage Mac OS X Server in their enterprise.

Configure Mac OS X systems to adhere to the same local policies you have in place for native Windows domain members. This is not to say that you would want to configure each server to have policies enforced by an Active Directory server (which could cause

Active Directory binding to break). To control access to the SMB service of Mac OS X:

- On the Access tab, uncheck **Allow Guest access**. Limit client connections to a reasonable number based on your server's capabilities. Uncheck the insecure authentication methods **NTLM** and **LAN Manager**.
- On the Logging tab, set **Log Detail** to at least **Medium**.

It is also possible to configure more granular security using the smb.conf file. For more information on configuring the Samba configuration file, please see:

Xgrid

Xgrid provides powerful mathematical processing by the use of grid-based computing. Using the Xgrid services it is possible to build large super-computer type environments. This is currently mostly used in academic environments but is gaining popularity in graphical environments as well. To maintain a high level of security when working with Xgrid:

- If you are using Xgrid, consider using Kerberos authentication when possible for all aspects of Xgrid.

Note: Many of the default open source packages included in Mac OS X are outdated and can be updated manually. Doing so can (and probably will) break the GUI controls that can be used in Server Admin. However, this will help to make the server more secure.

Note: When configuring shares in Server Admin remember that SMB, AFP and FTP are all enabled by default. For each share that you create only the required protocols should be enabled.

Password Maintenance

Having strong passwords, and changing those passwords regularly, is paramount for having a secure system. Fortunately, OS X provides tools for system administrators to enforce strong password policies, and tools for users to help them manage strong passwords

First, let's configure the system to enforce a password policy. To do this, you would use the pwpolicy command from the Terminal application. You need to open the Terminal application and perform a

```
man pwpolicy
```

… to fully understand all the features of the command. This command

```
sudopwpolicy –a <some admin user> –setglobalpolicy "minChars=8
maxFailedLoginAttempts=6 maxMinutesUntilChangePassword=129600
usingHistory=5 requiresAlpha=1 requiresNumeric=1"
```

… for example, will set a minimum length for passwords to 8 characters, an account will be locked after 6 failed login attempts, passwords will have to be changed every 90 days (129,600 minutes), you can't reuse the last 5 passwords, and your passwords have to have at least 1 number and 1 letter in them. Unfortunately, you can't require upper or lower case letters, or special characters. Also, it would seem that features change, depending on whether you are running OS X server or not. Some features require a password server. You can also change settings for a specific user as well with the "-u <user>" and "-setpolicy" options.

A lot of users struggle with creating a password that they can remember that also meets password security requirements. OS X' password assistant is designed to help. To get to the password assistant,

- Go to System Preferences
- Click on Accounts to get to Account Preferences
- Select your account on the left and click the "change password" button on the right.
- Click the key icon button to the right of the New Password field

From there you can choose different options to help you create a secure yet memorable password.

As a final note; a good security goal is to make passwords as long and complex as possible, without having users resort to writing them down, or taking other insecure shortcuts.

Safe Password Storage

Ideally, all passwords should be remembered. However, at times it may be better to use more secure passwords that might be difficult to remember. This can result in writing passwords down to assist in remembering them. For example, when concerned about a remote intrusion over a network, you might choose to store a physical copy of the password somewhere that you consider to be safe from a physical access standpoint. Generally speaking, it is better to create a password that can be remembered, even if it's a little bit weaker, and then changed or rotated more frequently when concerned about the strength of the password.

References

- http://research.corsaire.com/whitepapers/080818-securing-mac-os-x-leopard.pdf A Corsaire White Paper: Security Mac OS X
- http://www.apple.com/support/security/commoncriteria/ The Common Criteria Configuration and Administration Guide
- http://images.apple.com/server/macosx/docs/Leopard_Security_Config_20080530.pdf The Official Leopard Security Guide From Apple
- http://www.apress.com/book/view/9781590599891 Foundations of Mac OS X Leopard Security from Apress.

Appendix A

Last Updated: May 11th, 2025

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Abu Dhabi May 2025	**Abu Dhabi, AE**	**May 18, 2025 - May 23, 2025**	**Live Event**
SANS ICS418 Live Online May	**Gold Coast, QLD, AU**	**May 19, 2025 - May 20, 2025**	**Live Event**
SANS Thailand May 2025	**Bangkok, TH**	**May 19, 2025 - May 24, 2025**	**Live Event**
SANS Philippines SEC504 2025	**Manila, PH**	**May 19, 2025 - May 24, 2025**	**Live Event**
SANS Security Leadership Nashville 2025	**Nashville, TNUS**	**May 19, 2025 - May 23, 2025**	**Live Event**
SANS Dubai May 2025	**Dubai, AE**	**May 25, 2025 - May 30, 2025**	**Live Event**
SANS Madrid June 2025	**Madrid, ES**	**Jun 02, 2025 - Jun 07, 2025**	**Live Event**
SANS Baltimore Spring 2025	**Baltimore, MDUS**	**Jun 02, 2025 - Jun 07, 2025**	**Live Event**
SANS Cyber Defense Miami 2025	**Coral Gables, FLUS**	**Jun 02, 2025 - Jun 07, 2025**	**Live Event**
SANS Zurich June 2025	**Zurich, CH**	**Jun 02, 2025 - Jun 07, 2025**	**Live Event**
SANS Offensive Operations East 2025	**Baltimore, MDUS**	**Jun 08, 2025 - Jun 14, 2025**	**Live Event**
SANS London June 2025	**London, GB**	**Jun 09, 2025 - Jun 14, 2025**	**Live Event**
SANS OO East 2025: SEC535 Beta-2	**Baltimore, MDUS**	**Jun 12, 2025 - Jun 14, 2025**	**Live Event**
SANS ICS Security Summit & Training 2025	**Lake Buena Vista, FLUS**	**Jun 15, 2025 - Jun 23, 2025**	**Live Event**
SANS Amsterdam June 2025	**Amsterdam, NL**	**Jun 16, 2025 - Jun 21, 2025**	**Live Event**
SANS Cyber Defence Japan 2025	**Tokyo, JP**	**Jun 16, 2025 - Jun 28, 2025**	**Live Event**
SANS Paris June 2025	**Paris, FR**	**Jun 23, 2025 - Jun 28, 2025**	**Live Event**
SANS Rocky Mountain 2025	**Denver, COUS**	**Jun 23, 2025 - Jun 28, 2025**	**Live Event**
SANS Cyber Defence Canberra 2025	**Canberra, ACT, AU**	**Jun 23, 2025 - Jul 05, 2025**	**Live Event**
SANS Riyadh June 2025	**Riyadh, SA**	**Jun 28, 2025 - Jul 03, 2025**	**Live Event**
SANS Cloud Singapore June 2025	**Singapore, SG**	**Jun 30, 2025 - Jul 05, 2025**	**Live Event**
SANS Munich June 2025	**Munich, DE**	**Jun 30, 2025 - Jul 05, 2025**	**Live Event**
SANS Human Risk London July 2025	**London, GB**	**Jul 07, 2025 - Jul 09, 2025**	**Live Event**
SANS London July 2025	**London, GB**	**Jul 07, 2025 - Jul 12, 2025**	**Live Event**
SANS Riyadh July 2025	**Riyadh, SA**	**Jul 12, 2025 - Jul 17, 2025**	**Live Event**
SANSFIRE 2025	**Washington, DCUS**	**Jul 14, 2025 - Jul 19, 2025**	**Live Event**
SANS Amsterdam July 2025	**Amsterdam, NL**	**Jul 14, 2025 - Jul 26, 2025**	**Live Event**
SANS Anaheim 2025	**Anaheim, CAUS**	**Jul 21, 2025 - Jul 26, 2025**	**Live Event**
SANS DFIR Summit & Training 2025	**Salt Lake City, UTUS**	**Jul 24, 2025 - Jul 31, 2025**	**Live Event**
SANS Huntsville 2025	**Huntsville, ALUS**	**Jul 28, 2025 - Aug 02, 2025**	**Live Event**
SANS London August 2025	**London, GB**	**Aug 04, 2025 - Aug 09, 2025**	**Live Event**
SANS San Antonio 2025	**San Antonio, TXUS**	**Aug 04, 2025 - Aug 09, 2025**	**Live Event**
SANS Amsterdam May 2025	**OnlineNL**	**May 12, 2025 - May 24, 2025**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**