



OS X Security Set-up and Users Guide

George "Chip" Smith
FTG, HPCRD, CRD, LBNL



Introduction

Apple Computers have been very successful in the recent past with the OS X operating system. Scientists, researchers and users have begun to adopt these machines as their workstations and servers. It can be safely guessed that the number of these machines will only increase in the coming future.

Due to the uniqueness of the operating system, OS X is a UNIX based operating system. The underlying operating system is called Darwin, made up of two parts: the Mach Kernel and BSD subsystem. These two features allow for security features that are not present in the OS 9 legacy operating system. This document will cover critical points of security, common ideas and practices to be used in maintaining and keeping these systems secure.

The reference for this paper comes from two sources: Mac OS X security by Leon Towns-von Strauber and an newly unclassified document from the NSA (this document follows theirs). The NSA document is extremely rigid in the configuration of the OS X systems, however, that level and depth of the security used at that facility is not needed here at LBNL. All of the extra security measures that the NSA uses will not be discussed here.

Apple, Darwin, OS X, and BSD are trademarks and belong to the individual owners.

Target Audience

This document is mainly presented for system administrators/engineers and to users of a stand alone OS X computer. This document could be used with the server edition of the OS X, however, some settings and configuration would not be applicable. It also does not cover centrally administrated groups of systems. The reader is expected to have some knowledge of UNIX and OS X. The basic understanding of the reader in OS X is assumed. Some items will provide examples on usage.

This document should be read from beginning to end, and the reader is cautioned against skipping to the section they are looking for, as some later sections may refer to an idea or setting that is mentioned earlier in the documentation.

OS X Security Key Features

- A. Disabled root account: OS X, like other Unix Operating systems does have a root account, however, by default this is disabled. For any work that would need to be done on the system requiring root authority, administrative credentials (a person with administrative authorization) or sudo usage will be used. This greatly helps security and will allow for logging when a task needs to be completed by root. It should be standard practice that the root account remains disabled.
- B. Network services are disabled by default, even ssh. These services, including ssh server can be turned on. This will be discussed later.
- C. Keychain: This is a very important part of OS X security. The keychain mechanism will be used for an entire host of functions and maintains credentials and certificates that users will normally need to maintain by hand. All of these certificates and credentials are kept in an encrypted file and can only be accessed and read with proper authentication. An additional benefit is a user may have multiple keychains for managing different types of servers or accounts. They can be set to expire after a certain amount of time, re-authentication after a specified time or authenticating on each use of the particular keychain. If configured properly, this will give a strong security backing throughout the system.

Initial Set-up

2 Starting the machine

Initial screens:

- Welcome
- Personalize your settings
- Your Apple id. Select don't create an Apple id; continue.
- Registration Information: This is a do or don't. Users are reminded that information about them is being sent across the network in plain text to Apple. If the user is sensitive to this, this step can be skipped by pressing command – Q. In the “You have not finished setting up Mac OS X” window, click “Skip”.

2.1 Creating first account

2.1.1 This first account is the primary administrator account.

2.1.2 Enter a name. This can be any name, although, using the name “administrator” is easily guessable and should not be used. Make up a name.

Harriet, Popeye, etc.

2.1.3 Enter the short name for this account in the next box. Again, try not to use “admin” or something easily guessable. This is the name used to login to the account.

2.1.4 Enter the admin's password into the password and verify boxes. The password here should conform to LBNL guidelines for password structure. The password should be at least 10 characters and contain upper case, numbers and symbols, and it should not be a dictionary word. The password can be up to 255 characters.

2.1.5 One should leave the password hint box empty. The way this particular feature works is a user will get three attempts at the password and then this hint will be given. This hint may give an easy way for an unauthorized person to guess the password.

2.1.6 Click continue

2.2 Get Internet ready

This screen will only appear if the registration information was NOT skipped. You can select “I am not ready to connect to the Internet”. Click continue

2.3 Register with Apple

This screen will only appear if the registration information was NOT skipped.

Select register later, click continue

2.4 Select Time Zone

2.4.1 Select proper time zone (Pacific, Cupertino).

2.4.2 Click Continue

2.5 Set Date and Time

2.5.1 Select the ntp from time.Apple.com

2.5.2 Click Continue

2.6 Don't forget to register

2.6.1 If the registration screen was skipped, select “Done”.

2.6.2 Otherwise – Select register later; click Continue.

2.7 System Updates --!!! Extremely Important!!!

**** All security updates from Apple contain fixes for security issues. These are usually in response to known security problems. These are extreme critical ****

This will be one of the first pop-up windows that you will see during the initial setup, after the finder window.

You should run the update immediately. Your machine will be out of date by the time you are setting the machine up.

These updates will occur when there are new updates to be installed, and you will be notified by the same pop-up window that you see here.

It is HIGHLY recommended that you install these as soon as possible. To install these updates you will either have to use the administration credentials. Or, use your personal account credentials if they are sufficient to authenticate the update.

2.7.1 Agree to the license agreements that will pop-up.

2.7.2 Let the install finish

2.7.3 Click "Restart" after you have updated you will need to do this in almost all cases

2.8 Fixing file system permissions

While this step is not mandatory, it is recommended this be run after system updates and major installs. Users are cautioned that not doing this set of steps may introduce system instability and/or introduce new system vulnerabilities. If the user does not want to do this, the user should at the very least run this once a month after a security update. Should the system become unstable after an update (this has been observed), run this utility as soon as possible. Users should be able to contact a designated system engineer for a copy of the install disk required if it is lost. The key word in this section is "recommended".

NOTE: It is required that the user have a USB keyboard for this section. If a Bluetooth keyboard is being used during run time (the computer running in its normal fashion), the drivers for the Bluetooth functionality will NOT be loaded during this work and the Bluetooth keyboard will not function.

2.8.1 Insert Disk 1 of the install disks that came with your system.

2.8.2 When the gray screen with the Apple logo appears, press "C" and release.

2.8.3 Go to the menu bar that will appear, and select Open Disk Utility from the installer menu

2.8.4 Select the installation drive from the list of disk drives on the left of the Disk Utility screen.

2.8.5 Select Repair Disk Permissions button at the bottom of the First Aid screen.

Do not select "Disk Repair" in this menu.

2.8.6 Once that is finished, quit the disk utility by selecting the "Quit Disk Utility" under the Disk Utility menu.

2.8.7 Select "quit installer" under the installer menu Confirm you want to quit. The system will reboot and log into the administrator account.

2.8.8 Eject the disk.

3 Configuring System settings

The focus of this section is system wide configuration settings. It will include settings for the initial administrative account. Any text files that are mentioned in this section that will be edited need to be done as root. For users that are not familiar with “vi”, it is recommended that they use pico.

All the system configuration in this chapter will need to be handled by an administrative account (if the system was configured by the step in the proceeding section, the only account on the system at this point is an administrative one). Once automatic login has been disabled, one will be required to log in on the administrative account.

3.1 Removing the registration information

3.1.1 You should be logged in as an administrator, open the home folder.

3.1.2 If an alias named "Send Registration" is present, drag it to the trash.

3.1.3 Open the folder Library/Assistants under the home account of the first user (the administrative account).

3.1.4 If the file, “Send Registration” setup is present, drag it to the trash.

3.1.5 Choose Secure Empty Trash from the Finder menu to delete the files.

3.2 Managing System Preferences

System Preferences provides a way for a user and an administrator of the machine to define the way the computer behaves through a very handy graphical front end.

3.2.1 To start the program, click the Apple symbol in the upper left hand corner of the screen, then click System Preferences. The application will start in “show all” mode.

3.2.2 Desktop and Screen Saver:

The screen saver should automatically be turned on when the system is idle for a predefined amount of time. When used with requiring a password to wake from the screen saver or after the system has been “asleep”, it provides a good security layer to prevent unwanted use of the machine in the user’s absence.

How to set this will be under the section “other security settings”.

This preference screen allows for setting “hot corners”. This can be used to activate the screen saver when getting up from the machine. One can set this so if the cursor is moved to a corner of the screen it will carry out a desired action.

Setting a “hot corner” for the screen saver is highly recommended.

3.2.3 Security settings:

The security option found in the personal row of the system preferences application is extremely helpful in helping lock down the machine. This particular section has a section at the bottom for “All Accounts on this Computer”. The other settings in this panel only affect the current user and not all of the accounts on the machine.

3.2.4 Turning on encryption for a user directory (File Vault) will require the administrator account’s password. Configuring File Vault for individuals will be discussed later in setting up user accounts.

File Vault:

The File Vault utility on the Apple systems for encrypting home directories is a very strong and recommended way of protecting a user on the systems where physical security can not always be guaranteed, such as iBooks and PowerBooks. It should be highly recommended that the laptops have File Vault turned on, especially, with users who travel to foreign countries. This will help prevent any access to files should the laptop be lost or the hard drive being duplicated. In cases like this, the File Vault encryption is highly recommended for all accounts and users on the system. It should be noted that if a user is using disk intensive applications, such as video editing, the File Vault will impact disk performance.

There are two known times when this encryption can not guarantee confidentiality of a file. The first is when the file was created BEFORE File Vault was turned on. The second is in the trash folder. It is recommended that a person use “Secure Empty Trash” to ensure it has been properly removed from the hard drive.

Consider a file received or created after File Vault was turned on to be secure, A master password must be set before using the application to set encryption on user files. The master password can decrypt any user’s files on the system, which would be necessary if a user has forgotten their password. If this feature of the operating system is used it is highly recommended the “master password” does NOT match the administrators password for login to the system. When this is turned on it is also highly recommended that the system administrator/engineer keep the password on paper and store in a secure location. It is critically important that this password is not lost. The password should also meet the RPM guidelines of LBNL password usage.

3.2.4.1 Setting the master password: Select “Security” from the person preferences row in the system preferences application.

3.2.4.2 Unlock the window for editing, if necessary.

3.2.4.3 Select the master password button.

3.2.4.4 Enter the master password into the password field; verify it in the next box.

3.2.4.5 Do NOT enter anything in the hint field.

3.2.4.6 Select the OK button.

File Vault is now set to work with user accounts.

3.2.4.7 Next, set up the File Vault for the current user (the administrative account).

3.2.4.8 Click "Turn on File Vault". A dialog will open asking for the password.

3.2.4.9 Read the warnings that will pop up.

3.2.4.10 to continue, click "Turn on File Vault" or click cancel to stop. This will take some time to complete, and is directly related to how many files are in the directory. It should also be noted that the system will require all users to log out (if there are others logged in at this point, which shouldn't be), with the exception of the current account.

3.3 Additional Security Settings:

At the bottom of the panel there is "Require the password to wake this computer from sleep or the screen saver". This is only for the current person logged in and should be set for all users. The individual user can change this but they should set this option. The remaining settings affect all accounts on the system.

3.3.1 Click- show all icons on the system preferences. Or restart the system preferences if necessary.

3.3.2 Click the "Security" icon.

3.3.3 Check require password to wake this computer from sleep or the screen savers.

3.3.4 Unlock the window for necessary editing in this window.

3.3.5 Place a check in the box "Disable automatic logon".

3.3.6 Place a check mark in the box for "Require password to unlock each security preference".

3.3.7 The LOG out after <x> amount of inactivity should be Unchecked, for the following reasons: the automatic logout can quickly become irritating to the user, it will kill user processes that are currently running, and the log out process can fail because some applications will prevent this and require user intervention. It is better to have the system automatically spawn the screen saver after a certain amount of time.

3.3.8 Click the unlock icon at the bottom of the screen.

3.4 Bluetooth settings:

Bluetooth technology will be on most of the workstations and laptops. While this won't be disabled at this time at LBNL, there are several security concerns the user should be aware of.

3.4.1 If you are traveling to a high security Lab, this will have to be disabled.

3.4.2 Bluetooth is a "sniffable" technology. In short, this technology can act like a TTY sniffer by someone running proper software. This means that if a person with bad intentions does this, they will be able to read any passwords you type.

3.4.3 There are now viruses that can be transmitted to your machine using Bluetooth technology.

3.5 CDs and DVDs:

These should be set to not take any actions when media is inserted into the machine (on a currently account that is logged in). The idea behind these settings is that it is good practice that machine doesn't open a random CD or DVD, that may have unknown software on it that would normally automatically start.

3.5.1 In the system preferences application, click the CDs and DVD icon.

3.5.2 Pull down and select "ignore" when inserting a music cd

3.5.3 Pull down and select "ignore" when inserting a video cd.

3.5.4 Pull down and select "ignore" when inserting a video DVD.

3.6 Power settings:

This section is important because this will aid in protecting the computer when the user steps away from the computer or leaves for the evening. If the user forgets to lock the machine before leaving, the computer will be able to take care of this without intervention. This will protect the user from other people walking by from using there computer without permission.

3.6.1 Click the energy saver icon from system preferences.

3.6.2 on laptops, set the sleeping to 1 hour or less (to conserve battery life), on desktops, this can be set to never.

3.6.3 Set the check mark for the display sleep and set the slider for 15 minutes.

3.6.4 Set the check mark for put hard drive to sleep when possible on the laptops, this is optional on workstations.

3.6.5 Click the options tab in the panel.

3.6.6 Uncheck the wake from modem check box, this is not needed.

3.6.7 Check for wake for network Ethernet access by the administrator.

3.6.8 Re-starting after power failure is an option according to user preference.

3.6.9 Relock this panel.

3.7 Sound:

No configuration changes are need here.

3.8 Network settings:

No immediate configurations are needed here. The only ones that would be of interest are setting the ip address of the workstation. On laptops, setting both the wireless and network to DHCP will be needed. If it is a laptop, you can set for different locations.

It should be noted that if this is a laptop and the user will be traveling to high security labs, it will be necessary to uncheck Bluetooth and wireless connection prior to arriving at the lab, as these are generally not allowed at those labs. There is a location tab, which is rather handy for the laptops, the user or admin can set these according to their use of the laptop at home or other locations they frequently use the laptop at.

3.9 Sharing:

To its credit, Apple has made these services disabled by default. These services should generally remain disabled if they are not needed. The less services running, the better.

3.9.1 Personal File sharing: this will enable other users on other computers to see the content of the local user's public directory.

3.9.2 Windows Sharing: this is the use of SMBFS or CIFS protocol to allow windows machines to map the user's home directory. There are well known risks of using this service.

3.9.3 Personal Web Sharing: This service allows other users to browse the SITES directory over the Internet via a web browser. This should be disabled, unless this is a web server.

3.9.4 Remote Login: This should be enabled for users wishing to use the ssh and scp protocols.

3.9.5 FTP access: Disable this.

3.9.6 Apple Remote Desktop: Generally this is not used, however, users with an OS X administrator may use this feature. Contact your system admin about this.

3.9.7 Remote Apple Events: This should always be disabled.

3.9.8 Printer Sharing: This should be disabled. The Lab uses the cups printing system and the machine should be set to use the print servers.

3.9.9 The systems machine name should be set at this time. During the setup procedures described here, the machine name will assume the name of the first user doing the setup.

3.9.9.1 Click the sharing icon in system preferences.

3.9.9.2 Click on the services in the sharing panel.

3.9.9.3 Unlock the window for editing.

3.9.9.4 Make sure all boxes are unchecked with the exception of the remote login.

3.9.9.5 Replace the existing computer name with the new one in the "Computer Name" box.

3.9.10 Mac OS X provides basic firewall protection through the firewall tab in the sharing panel. It is highly recommended that is turned on. If "remote login" is enable you will see this box checked. Click the start button.

There is an ipfw command available under the terminal window. If there is to be UDP traffic, it may be necessary to use the firewall in this way.

3.9.11 Under the "internet tab" there is internet sharing. This should remain

disabled on all types of machines while at the lab, as this will create an access point for other computers to connect to and use the same Ethernet connection as this machine. The use of this function is generally not allowed under the policies of the Lab.

3.10 Accounts:

Accounts allow the system administrator to create accounts for other users on the system. It is also possible to create accounts under the “netinfo” application. It is highly recommended that all accounts to be made use this panel to add or remove users. Unless the user is very familiar with “netinfo”, use the account icon to add users. **The incorrect use of Netinfo can make the machine unusable.**

- 3.10.1 Click on accounts in the system preferences panel.
- 3.10.2 Click on the lock to unlock the panel if needed.
- 3.10.3 Click on “login options” to see general setting for user accounts.
- 3.10.4 Select “name and password” in the first section. This will cause the system to require an actual name and password to login to the machine. The other setting will cause the user name to be listed, which is not a good practice.
- 3.10.5 Uncheck login automatically if this is set.
- 3.10.6 Hide the Sleep, Restart, Shutdown buttons: this is by department policies.
- 3.10.7 Enable fast user switching. Policy by department, especially on certain shared machines.
- 3.10.8 Re-lock the panel at the bottom.
- 3.10.9 Date and Time settings:
- 3.10.10 Click “date and time” in the system preferences panel.
- 3.10.11 Unlock the panel if necessary.
- 3.10.12 Click set date and time automatically, the default setting is fine.
- 3.10.13 Click the save button.
- 3.10.14 Close system preferences.

4. Securing Initial System Accounts

At this point there are two accounts on the system that are going to need securing. The permissions on the home directory of the administrator account need to be changed. Any necessary modifications to the root account should be considered at this time. It should be noted that the root account and the administrator account are not the same thing on OS X.

4.1 Restricting the administrator’s home folder permissions:

When File Vault is not enabled on the administrator account (for example, on the workstations), it is possible for other users to browse this directory. To fix this, open a terminal window (or X-term) and run this command against the administrator directory, where <administrator> is the name of the directory of the administrator account.

sudo chmod 700 /Users/<administrator>

4.2 Securing the root account:

OS X is a Unix based operating system, and like other Unix systems, the root account is allowed to carry out any actions on the machine. Many administrative functions can be carried out by root on these systems and if there are multiple administrators taking care of items on the machine, the process of tracking who did what can become extremely difficult. OS X, by default during the install, leaves the root account disabled, making impossible to directly log in as root, and it is extremely recommended that this account remain disabled. By virtue of the keychain mechanism, administrative accounts will provide additional authentication when performing administrative functions. The force of authentication makes this set up a good way to help in security issues. If the root account has been enabled, this is the time to disable it again. Please follow these directions closely if you are unfamiliar with the “netinfo” application.

4.2.1 Log into the administrative account and start the “netinfo” utility you will find under /Applications/Utilities.

4.2.2 Click on users in the second column at the top of the “netinfo manager panel”. This will open a list of users in the third column.

4.2.3 Click on the root item in the user’s column. The root’s user properties and any other values will appear in a window below this.

4.2.4 Click on the lock to unlock this panel, Provide the administrator’s short name and password for unlocking.

4.2.5 If the property “authentication authority” is listed in the bottom of the window, click on it to highlight that property.

4.2.6 Go to the top of the window and click the “delete” icon to remove this property.

4.2.7 Double click the property associated with the “passwd” property located in that bottom property list. If there is an asterisk in the field the root password was never set, if it has been it will be a string of asterisks or a password hash.

4.2.8 Type a single “*” to replace this field.

4.2.9 Click on the locking icon to relock this panel.

4.2.10 When the “Confirm Modification” appears, select “Update This Property”

4.2.11 Quit the Netinfo Manager Application: The root account is now disabled.

4.3 Using *sudo*

The *sudo* application allows the system administrator to perform command line functions in the name of root. For more detailed information on the use of *sudo*, open a terminal window and type: “man *sudo*”.

The system uses a file called /etc/sudoers to determine who can use *sudo* and who can’t. The file is rather complex and one should open a terminal and type: “man *sudoers*”.

4.4 Securing Single User Boot

Like PC x86 based machines there is a way to set a password for the BIOS. However, since physical access to the machine is probable, and getting around this password is rather easy, this part will be left to the option of the user. There is, however, a way to require a password for root during the single user mode, and this should be done. To make this work, one will need to mark the console and the ttys as insecure in the file /etc/ttys. It will also require that one enters a password into the file /etc/master.passwd. This will make it rather difficult for someone to log in after booting into single user mode.

4.4.1 Log in as the system administrator.

4.4.2 Start the terminal application.

4.4.3 At the command line: `cd /etc/`

4.4.4 Make a backup of ttys: `sudo cp ttys BAK.ttys`

4.4.5 `sudo <vi, pico> ttys`

4.4.6 Replace all occurrences of the word “secure” with the word “insecure”.

Anything that does not begin with a “#” is a configuration line.

4.4.7 Exit, saving your changes.

For adding the password in /etc/master.passwd, `cd /etc/`

4.4.8 `sudo <vi, pico> master.passwd`

4.4.9 Within the editor delete the asterisk following the word “root”.

4.4.10 Open another terminal window, issue the following command line, where <xx> is two random characters, and <password> is an LBNL appropriate password. type:

```
openssl passwd -salt <xx> <password>
```

4.4.11 A hash will be displayed after this.

4.4.12 Type or paste this password hash into the place where you deleted the “*” in the other terminal window.

4.4.13 Exit, saving the changes.

4.5 Logon Warning Banners

Logon banner warnings should be set in the MOTD and a pop up window on all machines. These are the instructions for OS X.

The file you will edit is /Library/Preferences/com.Apple.loginwindow.plist . This will require you log on as the administrator of the machine.

4.5.1 Open the terminal program.

4.5.2 Open the file using vi or pico by typing:

```
sudo <vi,pico> /Library/Preferences/com.Apple.loginwindow.plist
```

4.5.3 Follow this closely: Immediately after the <dict> tag, add new lines with a <key> and <string> as shown below in bold. The new <key> tag MUST contain LoginwindowText, but the text should be the appropriate LBNL warning banner text.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN"
"http://www.Apple.
com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>LoginwindowText</key>
<string> *****
                NOTICE TO USERS
                -----
```

This computer is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

```
</string>
<key>PicturePathLW</key>
```

4.5.4 Exit, saving the changes, the next user login with the GUI will now see the

banner.

4.5.5 Edit /etc/motd and place the same text as above in this file.

4.6 Syslog configuration

It is required to have workstations send their syslogs to the centralized server at the lab. The following directions will enable this.

4.6.1 Open a terminal as the administrator.

4.6.2 `sudo vi /etc/syslog.conf`

4.6.3 Jump down to the end of the file and add this line: `*.* @syslog.lbl.gov`

4.6.4 Exit, saving your changes.

4.6.5 Send a hang-up signal to syslog to re-read its configuration. Type this in the terminal window:

```
sudo killall -SIGHUP syslogd
```

4.7 Optional Disabling of OS 9

While the use of the OS 9 part of the Apple is not prohibited, it is strongly recommended that this be disabled, unless there is a good business reason to have it enabled. OS 9 does not have nearly the amount of security features that OS X has, and should be avoided at all costs due to the security holes. The following instructions will explain how to remove this. Please follow these directions carefully or one could remove parts of OS X inadvertently.

4.7.1 Log into the administrator account.

4.7.2 Start a terminal

4.7.3 Type the following on the terminal command line:

```
sudo rm -rf "/System/Library/PreferencePanes/Classic.prefPane"
```

4.7.4 Type the following commands, in order, one at each prompt after the return of the command line after execution.

```
sudo rm -rf "/System/Library/Classic"
```

```
sudo rm -rf "/System/CoreServices/Classic Startup.app"
```

```
sudo rm -rf "/System/Library/UserTemplate/English.lproj/Desktop/Desktop (Mac OS 9)"
```

4.7.5 Type the following commands to remove additional OS 9 files in a terminal window. **!!! Follow this EXACTLY with the ticks, if you don't, you will remove the /System folder and then the machine will have to be re-installed!!!**

```
sudo rm -rf "/System Folder"
```

```
sudo rm -rf "/Mac OS 9 Files"
```

4.7.6 Type the following commands to remove any OS 9 applications on the system (if they exist). ***Again follow this EXACTLY, with the ticks.***

```
sudo rm -rf "/Applications (Mac OS 9)"
```

4.7.7 Restart the system.

4.8 Guidelines for creating user accounts

Accounts should never be shared. Each person on the system should have their own individual account. This should be the same for the administrators, if there is more than one. There are a number of reasons to have these rules, not to mention, that it is LBNL policy.

Individual accounts maintain a good accountability. If an account is shared, it will be difficult to track who did what action on the system.

Individual Administrative accounts would achieve that same accountability.

If the shared account becomes compromised, it is going to be hard to track, if it is ever noticed.

4.9 Creating User accounts

4.9.1 Start the system preferences application.

4.9.2 Click on the Accounts icon at the bottom of the panel.

4.9.3 Un-lock the new panel for changes.

4.9.4 To create an account, click the "+" button below login options.

4.9.5 Enter the name in the name account (Use first and last name), then add the preferred login name on the short name field. Choose a secure password and verify it in the next two fields, using LBNL password policies.

4.9.6 Leave the password hint field BLANK, do not use this feature.

4.9.7 Click the security button.

4.9.8 Make sure that the "Allow this user to administer this computer" is unchecked, if this is a user. If this is an administrative account, check this box.

Activating the File Vault can not be started at this time for the user (important on laptops). This will be covered later on in this section.

4.9.9 Repeat the above steps, starting with 4, to add more user accounts.

4.9.10 When finished re-lock the panel.

4.10 Securing user accounts

4.10.1 As the administrator, log in to the system

4.10.2 Open a terminal

4.10.3 Type this command:

```
sudo chmod 750 /Users/<username>
```

4.10.4 Repeat this for all users on the system, except for the administrator accounts (they should be set to chmod 700).

4.10.5 Close the terminal.

4.11 Enable system updates

4.11.1 As the administrator, log in to the system.

4.11.2 Start the system preferences application.

4.11.3 Click “Software Update”

4.11.4 Check for updates now (this may have been bypassed earlier).

4.12 Turning on File Vault for the user

4.12.1 Log in to the machine as the user.

4.12.2 Make sure all applications are closed, this will log out the user to accomplish the encryption.

4.12.3 Start the system preferences application, and click the “Security” icon.

4.12.4 Unlock the panel if necessary.

4.12.5 Click “turn on File Vault”

4.12.6 When prompted enter the password for the account when the account was created and click “OK”.

4.12.7 Click on the “Turn on File Vault” when it appears.

4.12.8 At this point the user will be logged out and the file encryption will proceed.

4.12.9 Repeat this process until all the user accounts have been fixed.

5. Understanding Keychains and Configuration

OS X has an application called Keychain Access. This is an application that stores collections of commonly used password and certificates. These passwords, certificates and any other private values (called secure notes) that are used by a person or an application are placed into a keychain and are encrypted. These stored values are then only accessible to the user via their keychain password.

A user can create multiple keychain using the application “Keychain Access”. Each keychain can store multiple values, with each value called an “Item”. A user

can create an “Item” to be placed in the keychain. When an application needs to store an item in the keychain, it will use the store it in the default keychain for the user called “login”. The user is free to change this.

It is commonly realized that when a user needs to remember a number of passwords, they will commonly use one password for multiple places. A common instance of this, is using the same password across multiple, non-linked machines and may be forced to write these passwords down. The use of keychains will greatly reduce the number of passwords a user must remember. This will facilitate the use of very complex or randomly generated passwords. It should be noted that there is an inherent disadvantage of using keychains. If the user chooses a password that is weak or easily guessable, and the machine becomes compromised through their account, all the passwords stored in a particular keychain become compromised as well. The rule is to use strong passwords that follow the LBNL guidelines.

Despite the disadvantages of keychains, they provide additional protection passwords, passphrases and credentials on the system. There are cases, such as digital signing e-mail messages, that the certificate must be stored in the keychains. The use of use keychains with applications and certificates must be weighed against the application, function and need to use it.

5.1 Keychain Access

Changing the keychain or modifying the contents of a keychain is done through the application called Keychain Access. This application can be found in /Applications/Utilities. To make managing the keychains easier it is highly recommended showing keychain status in the menu bar.

5.1.1 Login into the account of the user whose menu bar is to be modified.

5.1.2 Start the Keychains Application found in /Applications/Utilities.

5.1.3 Select “Show Status in Menu Bar” located under the “View” pull-down menu. This will place an lock icon on the menu bar which allow the user to lock and unlock keychains, quickly start “Keychain Access” and the system preferences or lock the screen.

5.1.4 Select “Change Password of Keychain Access “login”“ from the edit menu.

5.1.5 To prevent the login password from automatically unlocking the login keychain, change the password to something different the user’s login password. This will be the new password for this particular keychain.

5.1.6 From the Edit menu, select Change Settings for chain ...

5.1.7 Select “lock when sleeping”.

Inside the “Change Keychain Password” dialog box, click the “i” button in the lower left hand corner of the box. This will open a “Password Assistant” dialog box that provides assistance in choosing a strong password. Enter the current password in the “Current Passwords” box, and then enter a new password in the

“New Password” text box. The password assistant will help the user determine the strength of the password as they type it. It will show the quality measure and a visible bar that grows with the length of the password. The bar will also turn from the color red to green as the strength of the password grows. Use a password that turns this bar green or nears 100% strength and/or no warnings appear.

As mention earlier in this document, and in the above explanations the “Password Assistant” can be used to help create strong passwords anytime a password is needed, just not within the keychain access. To do this, open the keychain access application, and select “Change Password of Keychain x”, where x is any keychain. Then, select “i” in the lower left hand corner, and use the “password assistant” box to help create a password. Once a strong password has been achieved simply cancel the help and use the password where it is needed, and the keychain x password is not changed.

5.1.8 Configuration of Keychain items.

It is important that one look at each item contained in the login keychain. Each item can be individually configured to permit access by specified applications. The lower part of the window of the Key Access application there are tabs that can configure attributes for each item. Repeat the steps below for each item that you find in this window.

- Select an item in the currently selected keychain.
- Click on the “Access Control” tab to show the attributes of the currently selected item.
- The “Allow all applications to access this item” should NOT be checked. If it is any application accessing this value can use the credential with out asking if it should.
- **Setting the above item (or any other item within a keychain) to “Allow all applications to access this item” will cause any application to use the credential with out prompting or intervention. This setting should never be selected.**
- The “Confirm be allowing access” option should be selected. When set the user will be prompted when an application needs to access the item.
- Place a check in the “Ask for keychain access” box. With this option set, the user will be prompted for the password/passphrase before the application will receive the needed credential.
- The “Allow any application to access this item” should not be set unless it is needed for business reasons. If there are any applications that show up in the list, you can highlight them and

click the “Remove” button. Repeat until all entries have been removed.

5.2 Creating Multiple Keychains

When the initial account was created, the only keychain that is created is the login keychain. A user may create additional keychains, each of which can be configured independently. This functionality allows a user to create keychains for specific purposes.

As a good illustration for this ability, a user may want to group all of his email credentials in one keychain. It would very unpractical for the user to have to re-authenticate each time they want to check their email. A keychain could be created that would manage the credential using the login keychain or from an entirely separate keychain that would manage them on its own. Once setup, this would enable the ease of mail checking and any other application accessing this keychain to authenticate before using the credentials.

The following section will give guidance in setting up three keychains in a users account, each with a different amount of “accessibility”. The configuration should be good enough for an average user, demonstrate how to set them up, and give hands on experience in using the keychain application. Once the user becomes accustom to using the application, the user should be able to create additional keychains with ease.

5.2.1 Keychain example 1: Frequently accessed keychain.

The first keychain that will be examined is designed to protect credentials that are accessed frequently and automatically after the user logs into the machine. A great example of this is the email account password that is used when email is checked. If the keychain were set to expire after 5 minutes, the user would be required to enter the password each time they check their email. This would quickly become irritating. The keychain should be unlocked when the user logs in and should re-lock when the computer goes to sleep or when the user logs out. It should be also set so that only the application that requires the specific credential be unlocked for only the needed application.

1. Start the Keychain Access application
2. Select “New Keychain” from the file menu.
3. Select a location for the new keychain, this should be in the user’s home directory. It should default to the keychain directory, use this if possible.
4. Give this keychain a name and click “save”. In this example, mail_keychain might be appropriate.

5. Select a new password for this keychain, the password assistant can be used here by clicking the “i” at the bottom of the screen.
6. Click on “Show keychains” if needed.
7. Click on the newly create keychain to highlight it.
8. Select “Change Settings for keychain “mail_keychain”” ... from the edit menu.
9. Make sure that “Lock when sleeping” is checked off and that the “Lock after x amount of minutes” is not checked.
10. Any other credentials for mail access that may be in other keychains should be moved into this new keychain. This can be done using the “Cut” and “Paste” feature from the edit menu or by selecting an item that needs to be moved and dragging into this keychain. Keychain Access will prompt you for the password of the keychain you are moving an item from. Enter the password and click “Allow Once”. The item should now appear in the new keychain list and NOT appear in the original keychain.
11. Configure all items that now appear in your new keychain. Select an item in the keychain and click “Access Control”. You should make sure that “Confirm before allowing access” and “Ask for keychain password” are selected. Remove any entries that reference other applications from the access list that should automatically access these credentials. Repeat this step for any remaining items in this keychain.

5.2.2 Keychain 2: Moderately accessed credentials (e.g. Database access).

This keychain will be designed to show how to protect credentials that are accessed frequently and automatically whenever a user is using a particular application that needs to access a credential from a keychain. An example of this might be the access credentials needed for a database application for every for every query to the database. This example will illustrate a keychain behavior where authentication will be used at the beginning of the session and then need re-authentication on a periodic (e.g. every 15 minutes) basis rather than each time the user queries the database.

1. Start the “Keychain access” application, if needed.
2. Select “New Keychain” from the file menu.
3. Select a location for the new keychain, using the same place as in the last exercise.
4. Type a name for the new keychain in the “save as” box, then click create. In this example we will name it “database_keychain”.
5. Create a password for this keychain. Again, the password assistant can be used to help you.
6. Select “Change Settings” for the keychain “database_keychain”

from the Edit menu.

7. Make sure the “lock when sleeping” is checked and that “Lock after x minutes of inactivity” option is selected and, for this example, set it to 15.
8. As with the previous example, move any credentials from other keychains that contain credentials you need for this. Again, authenticate the move, select “allow once” and you will find that the item is now moved from the other keychain.
9. Configure all item in this keychain. Select an item in the list and click on “Access Control”. Make sure that BOTH “Confirm before Allowing Access” and “Ask for keychain password” are checked. Remove any other application from this that are listed and only allow the application needed this credential. Repeat this step until all items are configured.

5.2.3 Keychain 3: Infrequently accessed credentials (e.g. web credentials).

The example of this keychain will demonstrate a set of credentials that are accessed infrequently or a credential that should be authenticate for each access and need strict access control. The first thought a user might have is that it may seem absurd to use a keychain that needs to be authenticated each time it is used. If the user has a keychain to store all of these passwords, some of which might be randomly generated, and protect those credentials with a strong password or passphrase, the absurdity of this idea diminishes. It also protects the user from using simpler password for each account, having to write down all the passwords, using the same password over many sites. It can quickly be established that this is a worthwhile keychain to have around.

1. Start the “Keychain Access” application, if needed.
2. Select “New Keychain” from the file menu.
3. Select a location to store your keychain.
4. Type a name for this new keychain account, click save as and select create. You can name this “accounts_keychain”.
5. Create a new password for this keychain. Again you can use the password assistant for help at the bottom by clicking the “i”.
6. Select “Change Settings” for the keychain “accounts_keychain” from the Edit menu.
7. Make sure that “lock when sleeping” and “lock after x minutes of activity” is selected. Set this last option to 0 (zero). It should be noted that the user can not see any of the passwords contained in this keychain unless the user changes this value to 1 or higher.
8. Move any credentials that are web access type from other keychains into this keychain. You can use the “Cut” and “Paste” function or the “drag and drop” for this.

9. Configure all items in the list as we have done in the past two examples. Make sure that both the “Confirm before Allowing access” and “Ask for keychain access” are selected. If there are any other entries in the list remove them. Repeat this on all items in this keychain.

5.2.3 Setting the Default Keychain

As we covered earlier, any new items automatically saved to a keychain an application are stored in the default keychain, which is initially set to be the login keychain. It is good to note that the user can set ANY keychain to be default. The default keychain should be the one that is completely protected. The login keychain that we worked with earlier in this document can be used as the default keychain. If the user wants to use another keychain as the default keychain, the user must make sure that it secured the same way as the login keychain. To change the default keychain, the following directions will demonstrate how to do this. If the user is satisfied that the login keychain is fine, this part can be skipped.

1. Start the “Keychain access” application, if needed.
2. If the drawer showing the users keychains is not open, click on the show keychains icon to open it.
3. Click on the keychain that the user desires to be default.
4. Pull down the File menu and select “Make keychain “X” default”, where X is the keychain is the one selected in step 3.

5.2.4 Additional Notes about Protecting Keychains

On laptops, which can have difficult security issues, it is possible to store your keychains on a USB key. This gives the advantage of having separate piece of hardware to store security credentials. The idea for this is that it will require both the laptop and USB key to use the laptop and access the account, not to mention, having to know the passwords or passphrases to unlock the keychains.

To take advantage of this great security idea, the following directions will detail how to use a USB key to store keychains. We will need to move the existing keychains from the place where they are stored to the USB key and configure “Keychain Access” to know where to look for them. The default location of the keychain files in each users “Library/keychain” directory. Also be aware if you stored your keychain in any other location, as those will need to be moved too. These directions can be applied to any other location the user may want to use, such as a USB or Firewire drive.

Please follow these directions closely. This procedure will require the deletion of

parts of the keychain but not other parts. Again follow the directions closely.

1. Start the Keychain Access application.
2. If the drawer showing the keychains is not open, click on the “show keychains” icon to open it.
3. Click on the keychain to be moved to highlight it.
4. Pull down the Edit menu and select “change password for keychain “x””, where x is the keychain to be moved.
5. Click on the “Details” arrow to show more details about the keychain.
6. Make a note of the keychain location and click “cancel”.
7. Pull down the File menu and select “Delete keychain “x””; where x is the keychain to be moved.
8. In the window that appears on the screen, select “Delete References”. **Do not delete the files, only the references should be deleted.**
9. Open the folder containing the keychain as noted in step 6.
10. Copy the file to the USB key.
11. Drag the original file to the “Trash”.
12. Choose “Secure empty trash” from the finder menu to delete the file.
13. In the keychain access window, select add keychain from the File menu and open the keychain file that was moved. The keychain will then appear in the list of keychains in the keychain access application.

The system will now access the keychain from its new location.

Acknowledgements

Apple OS X 10.3 'Panther' security configuration Guide, SNAC, NSA, document number: I331-009R-2004, Guide Version 1.1

Mac OS X System Administration, Leon Towns-von Stauber, Consultant, 2003 LISA conference, San Diego, CA.

Juan Meza, HPCRD Department Lead