Global Information Assurance Certification Paper

Austin Harman
GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b, Option 1
February 11, 2004

Security of a Mac OSX Machine

Abstract:

As a computer technician for a university I work with many IBM format desktop computers, but the most challenging work I have done so far has been on Apple's Macintosh computers. I used to wonder what crazy individual created such a machine. I started technical support on the Macintosh machines knowing nothing, and with the help of the internet I have learned most everything I need to know over the past few years. I have found most of my information online, which is the best place I have found to get information for the Macintosh system. Now that I know more about the Macintosh, and since the release of Apple's new operating system, I have become quite fond of Macintosh. In fact I am currently working toward making my PowerPC G4 my primary machine for work. I have currently been looking into security information for the new Macintosh Operating System X, because of the concerns some of the faculty and staff have about the system being based on the UNIX operating system. The following are a few topics I will be discussing throughout the paper.

- Software Update Utility
- Secure Empty Trash
- File Vault
- Disk Copy
- Mac OSX, Hackers, and Viruses
- Usernames and Passwords
- Physical Security

Introduction:

Have you ever heard the saying, "The chain is only as strong as its weakest link!"? I believe this is true in the security of computers on a network. The goal of a hacker is to find a weak link in the system, and then attack in any means possible. The few simple security topics that I have found, I believe would very helpful for most Mac users. These topics focus mainly on the new operating system Apple is releasing with all their new machines, Mac OSX. Some of the topics are still valid for Macintosh user that are using the old system 9.2.2, but the "how to" direction will not be the same.

With experience working for an institute for higher education, most of these security topics would be great for either professors or students using Macintoshes. Most computers are widely accessible to anyone that walks in the door of any office. Also, their may be multiple users using one machine.

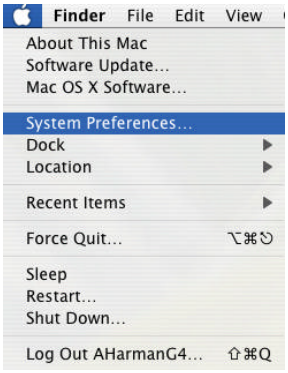
Apple Computer, Inc. states that Mac OSX, “delivers the highest level of security through the adoption of industry standards and open software development.”(Mac OSX Security, Apple Computer, Inc.) The way Apple makes this possible is by making their source code available to various users selected to testing all software over a period of time before being released. The people who test Apple’s software check for security problems within the program. If weaknesses or security holes are found, the software testers turn them back into Apple for repair. By using this open software development process, the programs can be fixed and released more securely without having to release as many software patches at later dates when the real damage is already done. This process also allows new software to be released at a quicker rate.

Software Update:

What happens if Apple does release some update or new software for my machine? How can I get it and keep my Mac patched for security purposes? Mac OSX comes with a built in Software Update utility! The Software Update utility downloads and installs new and updated versions of software available for the version of Mac OSX running on your machine. This includes operating system patches for the possible security problems found by Apple after the software was released on the market. Keeping your system software updated is very important because this creates a barrier for the virus writers and hackers, because of them trying to access your machine with security problems before they are fixed. To access and run the Software Update utility on Mac OSX, follow these steps:

1. Connect to the internet if not already connected

2. Choose “System Preferences” from the Apple menu



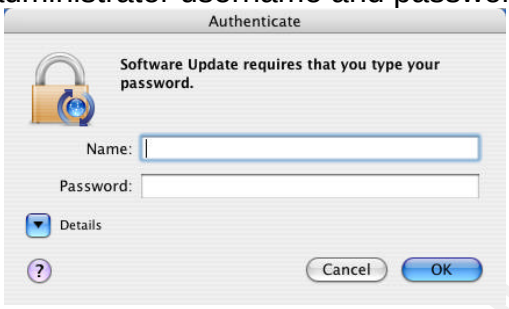
3. Choose “Software Update” icon from the System menu

4. Click “Check Now”

5. Select the items you want to install and/or update by clicking the check mark box next to the appropriate item

6. Click the “Install” button. You may have to click Agree to a license agreement if asked.

7. Enter an administrator username and password to the machine

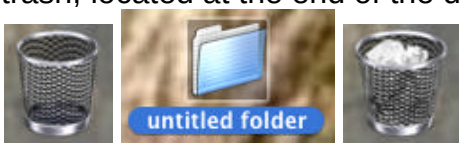


8. After the update is complete, the Software Update utility may ask you to restart the computer. If so, Click the “Restart” Button. If not, you can exit the Software Update utility.

Secure Empty Trash:

A new security feature of Mac OSX is the Secure Empty Trash command. On the previous versions of Macintosh operating systems, if you erased files and folder in the trash and then emptied the trash it would delete the files, but not permanently. If data recovery software is ran on the machine, it will retrieve the files and folders you thought were safely deleted. This is a local security problem if you have important documents that you do not want seen by other people. When emptying your trash on Mac OSX you can use the Secure Empty Trash command. By using this command, Mac OSX erases the data over the files and/or folders you have thrown away by writing meaningless data on the hard drive where these files and folders were stored. This permanently deletes these files and folders and makes them where they cannot be retrieved by any other means. There are only two easy steps for this to be accomplished.

1. Drag the files and/or folders that you want to delete **permanently** to the trash, located at the end of the dock

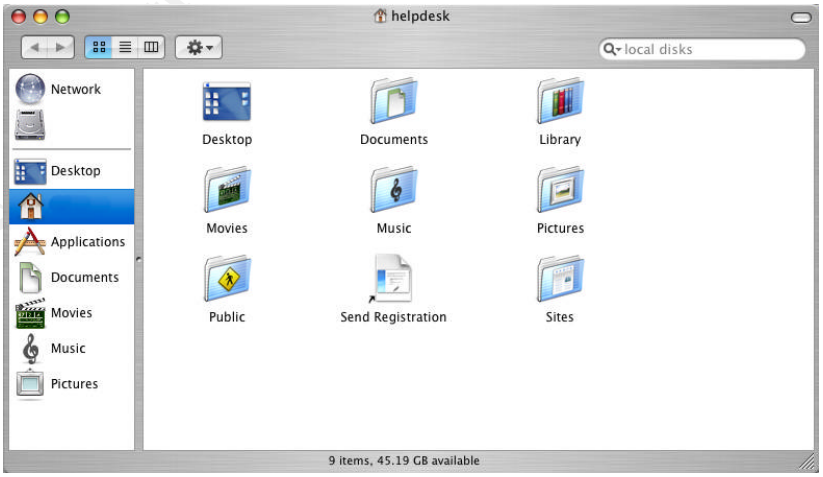


2. From the Finder menu, choose Secure Empty Trash

3. Click “OK” button to verify you want to **permanently** delete the files.

The FileVault:

A new security feature for Mac OSX is the FileVault system. FileVault is a built in file protection that has one of the most powerful encryptions that the government security standard allows. This encryption is the AES-128, the Advanced Encryption Standard with 128-bit keys. If you click on the Finder icon in the left side of the dock the finder windows will open. On the left side of the window there is an icon with a picture of a House that should already be highlighted, and it should have your computer name next to it. This is the area that acts as a folder or directory for files to be stored in. There is already some default folders inside this Home directory. This is where the FileVault creates its AES-128 bit encryption disk image for the files when FileVault is turned on.



A quick explanation of what the AES-128 bit encryption, as Apple Computer, Inc. gives, is if you compare the AES-128 with the DES-56, Digital Encryption

Standard at 56 bits, there are 10^{21} times more possible AES 128 bit keys than the DES 56 bit keys. Looking at this from another aspect, if you build a machine that can recover a DES key in a second, and then use the same machine to try and recover an AES key, it would take around 149 trillion years before it could finish. (Mac OSX FileVault, Apple Computer, Inc.)

Now, to keep you from getting to excited about the FileVault security. There has been a problem found with the FileVault and it has yet to be fixed, even with the new Panther update to 10.3.1. When you turn on the FileVault, your files are copied into a disk image with the AES-128 bit encryption. If there are files already in the Home directory when you turn on the FileVault it creates a copy of the files and puts them on this disk image and makes the disk image your new Home directory. It then erases the files from the original Home directory that does **not** have the AES-123 bit encryption. If recovery software is now ran on your machine it will find the old copy of the files that were there before turning on the FileVault. Therefore, the files that were there before turning on FileVault are not as secure as you thought they were. There are a couple of different ways you could fix this. The first one is what SecureMac.com has suggested to do; back up your data, write zeros to your hard drive, reinstall Mac OSX, turn on FileVault, copy your backed up data to the Home directory, and then get rid of your backup.(CodeSamurai, Mac OS X FileVault Security Advisory) Another way would be to back up your Home directory data, trash the Home directory data, execute the Secure Empty Trash command, turn on FileVault, copy backed up data to the Home directory, and then get rid of your backup.

The files kept in the Home directory are not accessed normally anymore. When trying to access the Home directory you will now be asked for either your login password or the master password. Access is not allowed locally on the machine, or through any network connections enabled on Mac OSX such as AppleTalk, FTP, Windows Sharing, etc., unless the password is entered.

Disk Copy:

Speaking of encryption, Mac OSX has also released a new feature utility called “Disk Copy”. Through Disk Copy you can make a virtual disk image that makes a Volume icon on the desktop. This volume is stored on the hard drive, and is encrypted and only accessed by your Keychain password. When this Keychain is unlocked you can put files and folders in the volume. When the Keychain is locked it takes the data you entered and encrypts it to where it can only be opened by the Keychain password. Now you can take this disk image which is in the format of a volume, which acts like an external disk, on your desktop and save it to floppy disk or e-mail it to someone. Now your data in that image can be safely transported physically or can be sent online. Whoever you are communicating with can now use the specified password and open the data.

Mac OSX, Hackers, and Viruses:

Since I have been working with Macintoshes, I have heard most Mac users say how protected their Macs are from viruses and hackers compared to a Microsoft Windows machine. This is not entirely true. Mac OS 9 for the most

part was protected from hackers and viruses because of how difficult and rare the operating system was to crack. Now that Mac has come out with their new and improved OSX they have opened themselves up to a world of insecurity. Mac OSX is based on the UNIX operating system which is much older than Microsoft Windows, and it is very familiar to the hackers because of the amount of time it has been around. People are still saying that the new Mac OSX is more secure than any other machine running any other type of OS. The reason for this is because there are many more Microsoft Windows machines than Mac OSX machines. Therefore, hackers and people who write viruses are most of the time looking for a majority to attack. Mac OSX machines are increasing in numbers very quickly though.

Keep yourself safe! Install anti-virus software for Mac OSX on your machine and make sure your virus definitions stay up to date. If you are not already behind a firewall, then you need to install some type of personal firewall on your system. Also, make sure that your current operating system is up to date by running the Software Update utility. None of these things can keep you one-hundred percent safe, because there is always someone that will eventually find a way though a security hole. The chances of this are slim as long as you keep your software and virus definitions updated.

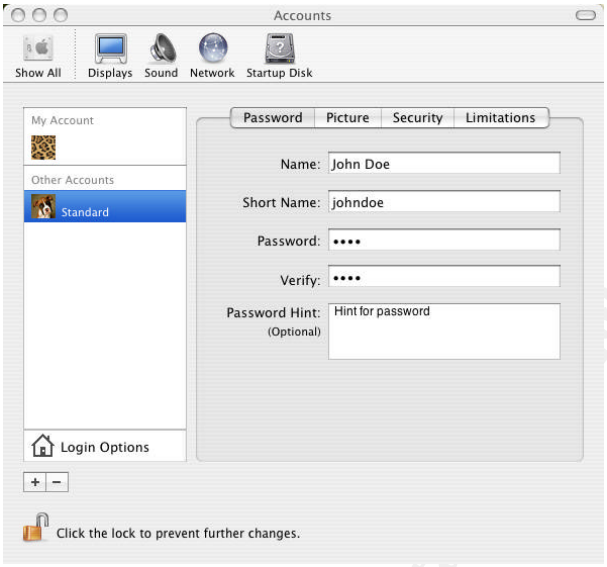
Usernames and Passwords:

Mac OSX is a multi-user operating system. Multi-user in this case means that multiple people can login to the Mac, and have their own Home directory and personal settings. If you recall the information about the FileVault above you know that you can encrypt your data in the Home directory. Using this multi-user environment creates a basic security for your files and folders. No one else can view your files and even if they try to retrieve your files, they are encrypted and cannot be accessed unless they know the password to your FileVault. Now, if you have a Mac OSX machine that multiple people need to use, a separate username and password account can be created for each of them to have their own profile. Use the following directions and notes to create a new user for Mac OSX.

1. Choose “System Preferences” from the Apple menu

2. Choose “Accounts” from the System menu

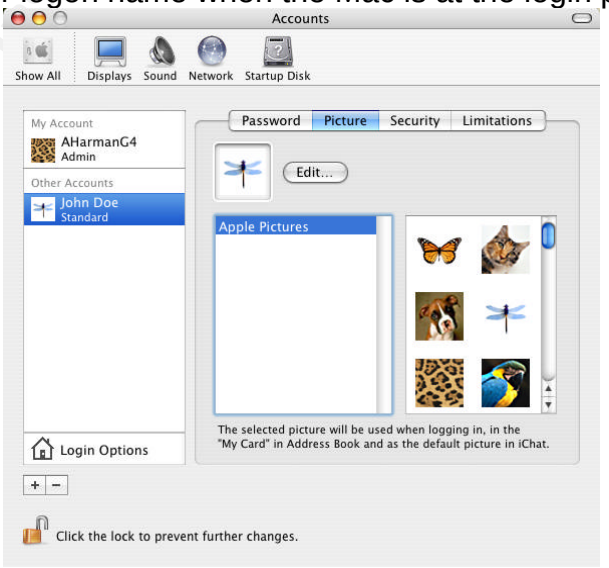
3. Click on the "+" button at the bottom left hand part of the menu to create a new user.



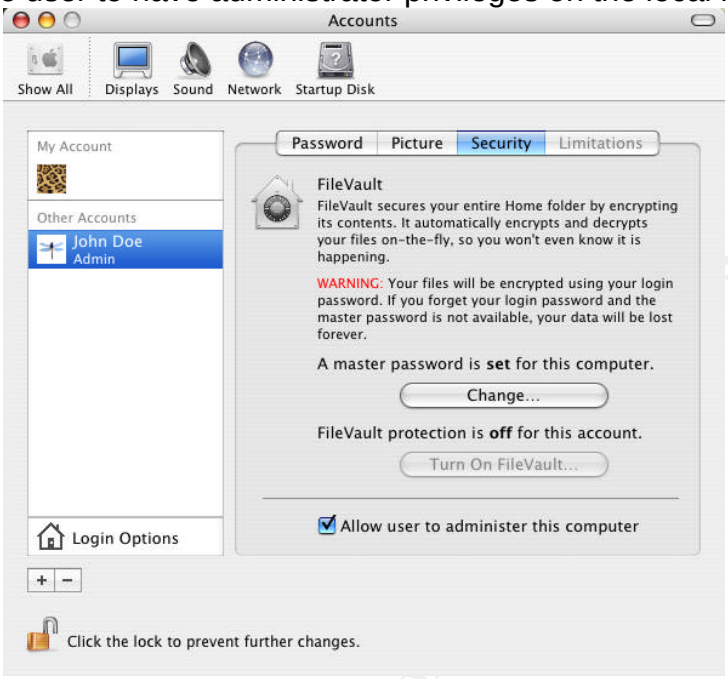
4. In this window under the "Password" tab enter the following:

- Name: Type in the name of the user
- Short Name: Type in a shorter name of the user (first name)
- Password: Type in a password
- Verify: Type in the password again to verify
- Password Hint: If you want, type in a hint to remind you of your password. If a person tries to login to your account and the password is typed in wrong the first time, this hint will be shown. So, be sure not to put the actual password or too easy of a hint in this box.

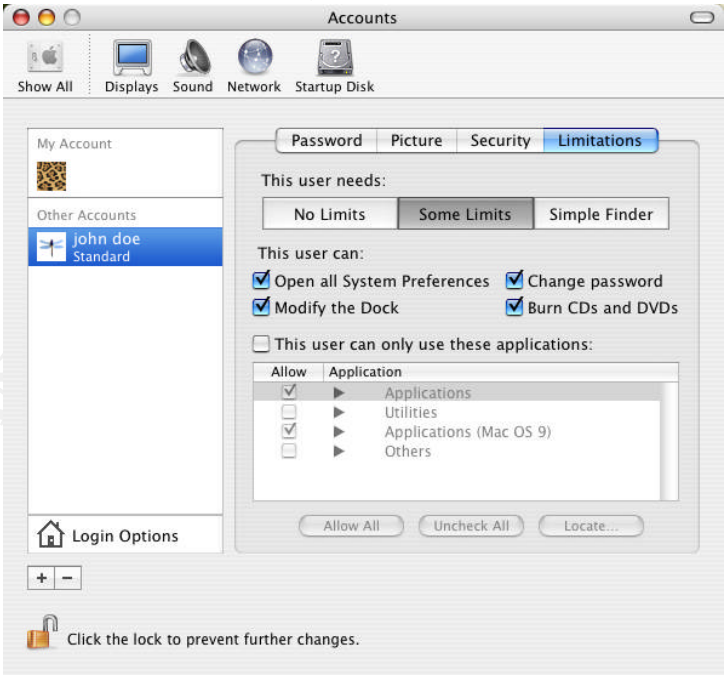
5. Under the "Picture" tab you can select various picture that will show up by your logon name when the Mac is at the login prompt



6. Under the “Security” Tab you can select the check box at the bottom for the user to have administrator privileges on the local machine.



7. Under the “Limitations” tab if you do not make the user an administrator you can select various limitations and customize the user’s ability of using the machine.



Physical Security:

On a Macintosh machine, I believe the most important type of security is physical security. Apple has made so many great physical security upgrades to

Mac OSX as talked about above. Mac OSX is still not perfect, even with their physical security. Apple has already released many vulnerability alerts for the Mac OSX machines. The best place I have found to find these type of alerts are at the securemac.com website. An example of one is if you have a certain type of USB keyboard, other than the apple keyboard, you can hold down Ctrl C, which is used to boot to a CD, and boot Mac OSX up. After a certain period of time it will bring you to the administrative root shell prompt caused by the init crashing. Init is a part of the kernel image. Apple claims that this is current in the Mac OSX 10.2.8 and earlier and the only way they know of fixing the problem at this time is to upgrade the init.c to the Mac OSX 10.3 init.c. Another example of a physical security hole that Apple has released is a problem with the screensaver password on Mac OSX. If you type in a series of keys in the keyboard before the password box comes up, the desktop will come up as a normal user of the computer. As a result, files and applications can be accessed and deleted. I have found no fix for this problem at this time.

Conclusion:

As a whole, the Mac OSX is a very secure platform. Remember to keep all items updated, most of all; the operating system, anti-virus, and firewall. Throughout this paper I have talked about the defense-in-depth system. Ask yourself this question! What can I do to protect my network/machine from attacks? As already mentioned above, the three main answers to this question are the following: anti-viruses, personal firewalls, and keeping your operating system and software patched. We also need to keep in mind the aspects of a secure network, which are confidentiality, integrity, and availability.

- Confidentiality – Making sure that secret data stays secure and confidential. This is what Apple is accomplishing with their Secure Empty Trash, FileVault and Disk Copy utilities talked about above.

- Integrity – The individual identification. As in the password protected FileVault system on the Home directory, and the encrypted data of the Disk Copy utility.

- Availability – The access to whatever is needed will be available to users at all times it is needed.

All items above have been used in the discussion throughout the paper. I feel the information in this paper would be very helpful for the basic Macintosh user. This will familiarize them with the basics of security on theMac operating system currently on the market, which is Mac OS 10.3, also called Panther. All screenshots and directions in this paper have been made with my Mac PowerPC G4 running Mac OSX 10.3.2.

Works Cited

Apple Computer, Inc. FileVault. 2004 <http://www.apple.com/macosx/features/filevault/>

Apple Computer, Inc. Get the Latest Updates. 2004 <http://www.apple.com/macosx/upgrade/softwareupdates.html>

Apple Computer, Inc. Safe and Sound. 2004 <http://www.apple.com/macosx/features/security/>

CodeSamurai. Mac OS X 10.3 Panther Screen Lock Bypass. 28 Oct. 2003 <http://www.securemac.com/macosx-screenlock-bypass.php>

CodeSamurai. Mac OS X FileVault Security Advisory. 6 Nov. 2003 <http://www.securemac.com/macosx-filevault-advisory.php>

Cole, Eric; Fossen, Jason; Northcutt, Stephen; and Pomeranz, Hal. SANS Security Essentials with CISSP CBK (Volume One). The SANS Institute, 2003

Cole, Eric; Fossen, Jason; Northcutt, Stephen; and Pomeranz, Hal. SANS Security Essentials with CISSP CBK (Volume Two). The SANS Institute, 2003

Hutton, Paul. Adding Users to OSX. 8 April 2003 <http://www.ucs.ed.ac.uk/usd/iss/ol/os/mac_osx/advanced/adding_users.html>

Sellers, Dennis. Hackers, Viruses, the Mac, and OS X. 6 Aug. 2001 <http://maccentral.macworld.com/news/2001/08/06/hacker/>

Storm, Jason. Mac OS X USB Keyboard Root Access. 31 Oct. 2003 <http://www.securemac.com/macosx-usbkeyboard-root.php>

Symantec Corporation. Protect your Mac on the Internet. 2004 <http://www.symantec.com/mac/security/open_door.html>