Securing an Apple OS X System

Alex Smith
Junior Information Security Analyst
UCIT Office of Information Security
5/7/2013

Table of Contents
Configure OS X Settings ................................................................. 1-3
  Creating a Strong Password .......................................................... 1
  Update Apple .................................................................................. 1-2
  Security Settings ............................................................................ 2
  Configure Your Firewall ............................................................... 2
  Setting up Folder Sharing ............................................................. 3
  Network Security Settings ............................................................ 3
Installing Security Software ............................................................. 4-5
  3rd Party Anti-Virus ....................................................................... 4
  Anti-Malware Software ................................................................. 4
  Encryption Software ..................................................................... 5
Securing Your Internet ................................................................. 5-6
  Securing Safari Settings .............................................................. 5
  Which Browser(s) to use ............................................................. 6
Post-Configuration Clean-up .......................................................... 6
  System Back-Ups .......................................................................... 6
References .................................................................................... 7
Operating System: Mac OS X 1.6 (Snow Leopard)

Notes: This Guide was made using Mac OS X 10.6 (Snow Leopard). Some settings and features may vary slightly for older (or newer) apple operating systems.
Physical security of your system should be the number one priority. No system is safe if it is stolen or accessible by others. Do not leave your laptop unattended. Use locks for containers which your system may be in (cars, rooms, lockers). When a system is left unattended in a safe location, it is best practice to lock your computer to the logon screen so that others may not access your system without a password. Make sure to do this when friends and family are present too. Anyone may be curious, and events such as “Facebook status hacking” are preventable.
A useful function in Apple OS X is the apple button. Go to the Desktop navigate to the top left corner. There is an Apple Icon which can be used to navigate to most directories on a Mac.
Configure OS X Settings

Creating a Strong Password

The first (and most important) step to securing Apple OS X is to make a strong password.

1. Begin by navigating to the apple and select System Preferences.
2. Under Systems Select Accounts, then click Users (left panel).
3. On the left select your account.
4. Select Change password…
5. Create a new password using the following criteria:
   - Length of 8-16 characters
   - Use at least 3 of the 4 following character sets:
     - Uppercase Alphabetic Characters
     - Lowercase Alphabetic Characters
     - (2 +) Numeric Characters
     - Special Characters (!@#$%^&*)

(When adding a Password hint, make sure it is useful but not too revealing.)

Update Apple

The second step to securing Apple OS X is to make sure the operating system is up to date. Apple OS X updates provide patches for security holes and vulnerabilities. These are released on a regular basis.

1. To apply updates, go the apple.
2. Select System Preferences, then click Software Update
3. Check the Check for updates box, select daily from the drop down menu, and make sure Download updates automatically is checked.
4. Select Check Now to update your system immediately.
Security Settings
1. Navigate to the apple and select System Preferences, then click Security.
2. Check the Require password box and select immediately from the drop down box.
3. Click the lock on the bottom left to make changes to the other settings. (Enter your password)
4. Check the following boxes: Disable Automatic Login, Use secure virtual memory, and Disable Location Services.

Configure your Firewall
1. Navigate to the apple and select System Preferences, then click Security.
2. On the center menu select Firewall.
3. On the bottom left of this menu select the Lock to make changes (enter your password).
4. Select Start to turn the firewall on.
5. Now select Advanced… near the bottom right of the menu.
6. Make sure that none of the three boxes are checked.
Setting up folder sharing:
If you want to share files with other computers on your home network you will need to set up a shared folder/folders.

1. Navigate to the apple and select System Preferences, then click Sharing.
2. From here you can add which files/folders you would like to share, to whom you would like to share them with, and their permissions to those files.
3. It is not recommended to share all files with all users as this may present risk you those files if their account is compromised.

Network Security Settings
1. Navigate to the apple and select System Preferences, then click Network.
2. Make sure the Ask to join new networks box is checked.
3. Now select Advanced… near the bottom right of the menu.
4. Check the boxes that say: Create computer – to – computer networks and Change networks boxes to require administrative approval.
5. Click OK.
Installing Security Software

Third Party Antivirus Software
There are many choices for 3rd party antivirus software. There are many free and many paid ones, the one you choose is up to you. Well-known suites include Avira/Avast/Comodo (Free), or Norton/McAfee (Paid). You may want to search the web for one that meets your needs (cost vs. security vs. performance). This guide will show you how to secure a computer with McAfee (free for UC students, faculty, and staff). If you choose to use a different security suite, use similar settings.

1. Open up your browser, go to http://www.uc.edu/ucit/ware/software/mcafee.html.
2. From there select the link under “Then, download the software”.
3. Update McAfee, then perform the initial scan, and then the rest should be good to go. For additional support consult the software website forum.

Anti-Malware Software
Anti-Malware Software is not necessary for Mac OS X. The reason behind this is that the Mac OS does not use a registry type system, therefore adware/spyware/malware cannot infect the system this way.

Encryption Software
Encryption software is very important for ensuring that physical access to hardware is difficult unless one knows the code to access it. Encryption is especially important for portable hardware such as external hard drives, laptops, and USB drives.

Attention: UC Faculty and Staff must use encryption software required by their department/college.
Mac OS X comes with FileVault encryption software pre-installed.
Here is how to activate it:
1. Navigate to the apple and select System Preferences, then click Security.
2. On the center menu select FileVault.
3. Select Turn On FileVault…
4. You will be prompted to set a Master Password, do this (remember how to make a secure password)
5. A warning prompt will display. Check the Use secure erase box and then select Turn On FileVault.
Here are a few third-party encryption software programs:

- AutoKrypt
- Privacy Drive
- Truecrypt

### Securing Your Internet

#### Securing Safari Settings

1. Open Safari
2. On the top menu select **safari**, from the drop down select **preferences**.
3. Select the **Autofill** tab and ensure the **User names and passwords** box is **unchecked**.
4. Select the **Security** tab the following boxes should be **checked**:
   - Warn when visiting a fraudulent website,
   - Enable Plug-ins,
   - enable Java,
   - Enable JavaScript,
   - Block pop-up windows,
   - Accept cookies = Only from sites I visit, Ask before sending a non-secure form from a secure website.
**Browser(s) to Use**

Choosing a web browser is almost entirely a matter of opinion. Some browsers are more secure than others and some are faster than others.

The prominently used web browsers for Mac OS X are Safari, Mozilla Firefox, Microsoft Internet Explorer, and Google Chrome. You can see a selection of the top ten browsers and how they are rated [here](#).

Internet explorer is currently recommended for security purposes and Chrome for usability. Most browsers are available free online. Just open Safari and go to the appropriate website to download one.

**Post-Configuration Clean-Up**

**System Back-Ups**

It is highly recommended that you make a back-up of your system and update it on a regular basis. Doing so will limit the amount of data that is lost in the case that your hard drive crashes or is physically destroyed. To do so you will need an external device that is the same size as or larger than your internal hard drive.

**Attention:** UC Faculty and Staff must backup systems as specified by department/college. (Frequency/location).

Here is how to use Mac OS X Time Machine:

1. Navigate to the **apple** and select **System Preferences**, then click **Time Machine**.
2. For this step you will need an **additional** internal/external hard drive connected to your system.
3. Select **Set Up Time Machine**.
4. Click the **lock** on the bottom left, Select **Backup Disk**…, then turn the **Time Machine** **ON**.
5. From here decide whether you want to **Set Up Time Capsule** (recommended(this will create constant restore points)) or **Use for Backup** (Backing up must be done manually).

Another way to regularly backup data onto an external device is to manage the process with third-party software. (Sometimes external devices come with such software).

You can try one of these:

- [Smartsync-Pro](#)
- [Stellar Drive Clone](#)
- [Wondershare](#)
REFERENCES:

CNET Downloads
Auto Krypt - http://download.cnet.com/AutoKrypt/3000-2092_4-75864366.html
TrueCrypt - http://download.cnet.com/TrueCrypt/3000-2092_4-10527243.html
Privacy Drive - http://download.cnet.com/Privacy-Drive/3000-2092_4-75752636.html
Smartsync Pro - http://download.cnet.com/SmartSync-Pro/3000-2242_4-10050564.html
Stellar Drive Clone - http://download.cnet.com/Stellar-Drive-Clone/3000-2242_4-75375355.html
Wondershare - http://download.cnet.com/Wondershare-Data-Recovery/3000-2242_4-75871233.html

Create Strong Passwords

Mac OS X Basic Security Settings
OIT Security and Assurance University of Minnesota
http://www.oit.umn.edu/prod/groups/oit/@pub/@oit/@web/@security/documents/content/oit_content_248495.pdf

Mac OS X Security Configuration Guidelines
Apples Official Security Guidelines
https://ssl.apple.com/support/security/guides/

Macworld
Encrypt files for safety
http://www.macworld.com/article/1053658/decmobilemac.html

Setup Windows 7 Securely - UCIT Office of Information Security
http://www.uc.edu/content/dam/uc/infosec/docs/general/Setup_Windows_7.pdf

SourceForge
http://www.sourceforge.net/

Tech 90
Password Evaluator
https://www.tech90.com/tools/password-evaluator/

TopTenReviews.com
Encryption Software Review
http://encryption-software-review.toptenreviews.com/