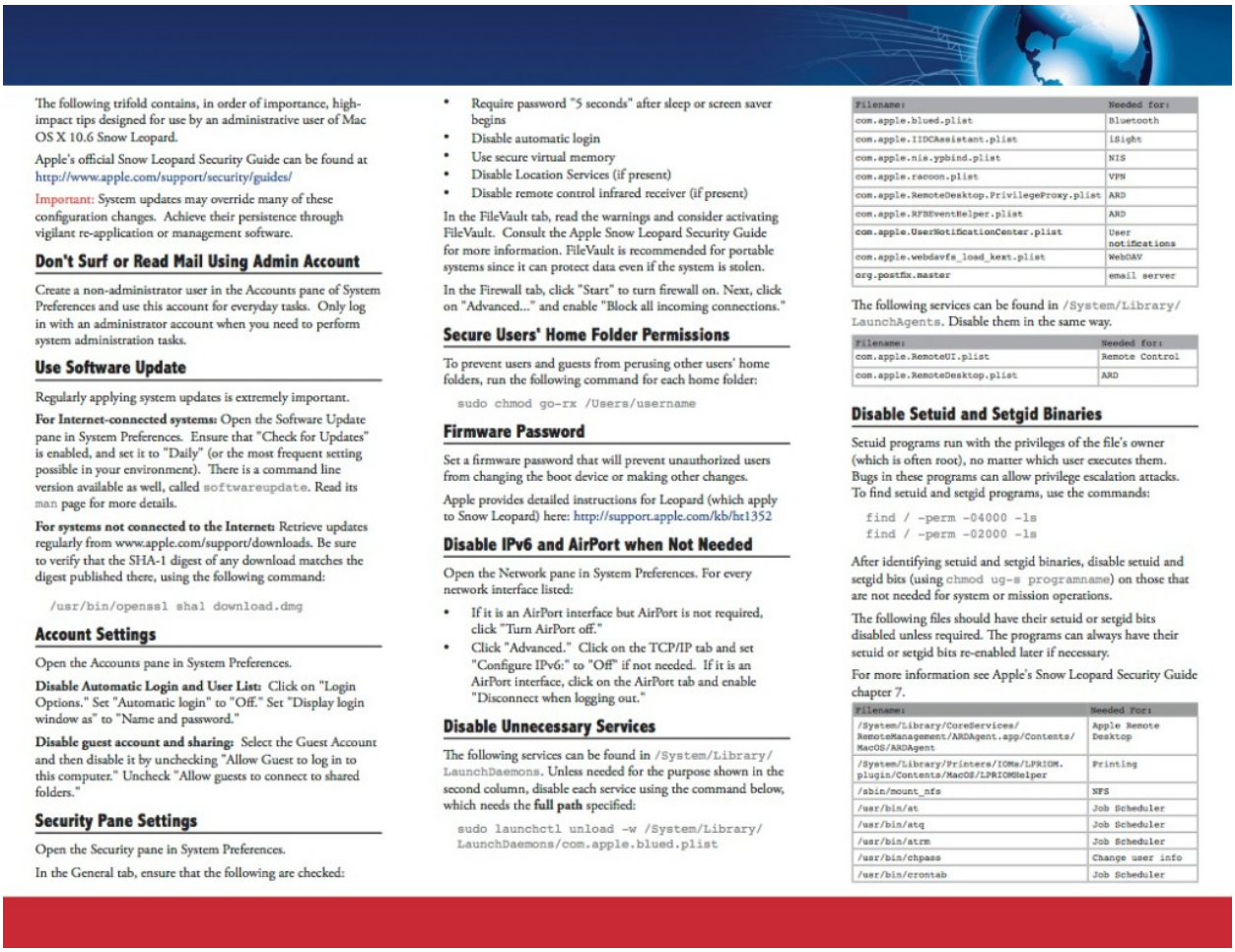
Take Your Mac OS X Security to NSA Standards
June 19, 2014
by Larry Chafin

Forword

While doing research for another article, I came across NSA's security setup for Mac OS X. No, the information gained was not from a clandestine hack, or some form of Wiki-Leaks. All the data you see here is readily available from the public version of NSA's website. We will be discussing a document that appears to have been designed as a three-fold double-sided pamphlet. Though this document may resemble a "Quick Start Guide", don't let its diminutive size lead you astray, there is a lot of information about how the NSA wants processes and settings used on their Mac OS X computers. Sadly, their instructions are a bit dated, as the latest document for this topic is for Snow Leopard, 10.6; however, many of their processes and settings are still viable, making further investigation worthwhile. So that you may refer to them, the NSA Pamphlet, entitled "Hardening Tips for Mac OS X 10.6 'Snow Leopard'", can be seen in Figure 1 and Figure 2, below.



The following trifold contains, in order of importance, high-impact tips designed for use by an administrative user of Mac OS X 10.6 Snow Leopard.

Apple's official Snow Leopard Security Guide can be found at http://www.apple.com/support/security/guides/

Important: System updates may override many of these configuration changes. Achieve their persistence through vigilant re-application or management software.

Don't Surf or Read Mail Using Admin Account

Create a non-administrator user in the Accounts pane of System Preferences and use this account for everyday tasks. Only log in with an administrator account when you need to perform system administration tasks.

Use Software Update

Regularly applying system updates is extremely important.

For Internet-connected systems: Open the Software Update pane in System Preferences. Ensure that "Check for Updates" is enabled, and set it to "Daily" (or the most frequent setting possible in your environment). There is a command line version available as well, called `softwareupdate`. Read its `man` page for more details.

For systems not connected to the Internet: Retrieve updates regularly from www.apple.com/support/downloads. Be sure to verify that the SHA-1 digest of any download matches the digest published there, using the following command:

```
/usr/bin/openssl sha1 download.dmg
```

Account Settings

Open the Accounts pane in System Preferences.

Disable Automatic Login and User List: Click on "Login Options." Set "Automatic login" to "Off." Set "Display login window as" to "Name and password."

Disable guest account and sharing: Select the Guest Account and then disable it by unchecking "Allow Guest to log in to this computer." Uncheck "Allow guests to connect to shared folders."

Security Pane Settings

Open the Security pane in System Preferences.

In the General tab, ensure that the following are checked:

- Require password "5 seconds" after sleep or screen saver begins
- Disable automatic login
- Use secure virtual memory
- Disable Location Services (if present)
- Disable remote control infrared receiver (if present)

In the FileVault tab, read the warnings and consider activating FileVault. Consult the Apple Snow Leopard Security Guide for more information. FileVault is recommended for portable systems since it can protect data even if the system is stolen.

In the Firewall tab, click "Start" to turn firewall on. Next, click on "Advanced..." and enable "Block all incoming connections."

Secure Users' Home Folder Permissions

To prevent users and guests from perusing other users' home folders, run the following command for each home folder:

```
sudo chmod go-rx /Users/username
```

Firmware Password

Set a firmware password that will prevent unauthorized users from changing the boot device or making other changes.

Apple provides detailed instructions for Leopard (which apply to Snow Leopard) here: http://support.apple.com/kb/ht1352

Disable IPv6 and AirPort when Not Needed

Open the Network pane in System Preferences. For every network interface listed:

- If it is an AirPort interface but AirPort is not required, click "Turn AirPort off."
- Click "Advanced." Click on the TCP/IP tab and set "Configure IPv6:" to "Off" if not needed. If it is an AirPort interface, click on the AirPort tab and enable "Disconnect when logging out."

Disable Unnecessary Services

The following services can be found in `/System/Library/LaunchDaemons`. Unless needed for the purpose shown in the second column, disable each service using the command below, which needs the **full path** specified:

```
sudo launchctl unload -w /System/Library/
LaunchDaemons/com.apple.blued.plist
```

Filename:	Needed for:
com.apple.blued.plist	Bluetooth
com.apple.IIDCAssistant.plist	iSight
com.apple.nis.ypbind.plist	NIS
com.apple.racoon.plist	VPN
com.apple.RemoteDesktop.PrivilegeProxy.plist	ARD
com.apple.RFBEventHelper.plist	ARD
com.apple.UserNotificationCenter.plist	User notifications
com.apple.webdavfs_load_kext.plist	WebDAV
org.postfix.master	email server

The following services can be found in `/System/Library/LaunchAgents`. Disable them in the same way.

Filename:	Needed for:
com.apple.RemoteUI.plist	Remote Control
com.apple.RemoteDesktop.plist	ARD

Disable Setuid and Setgid Binaries

Setuid programs run with the privileges of the file's owner (which is often root), no matter which user executes them. Bugs in these programs can allow privilege escalation attacks. To find setuid and setgid programs, use the commands:

```
find / -perm -04000 -ls
find / -perm -02000 -ls
```

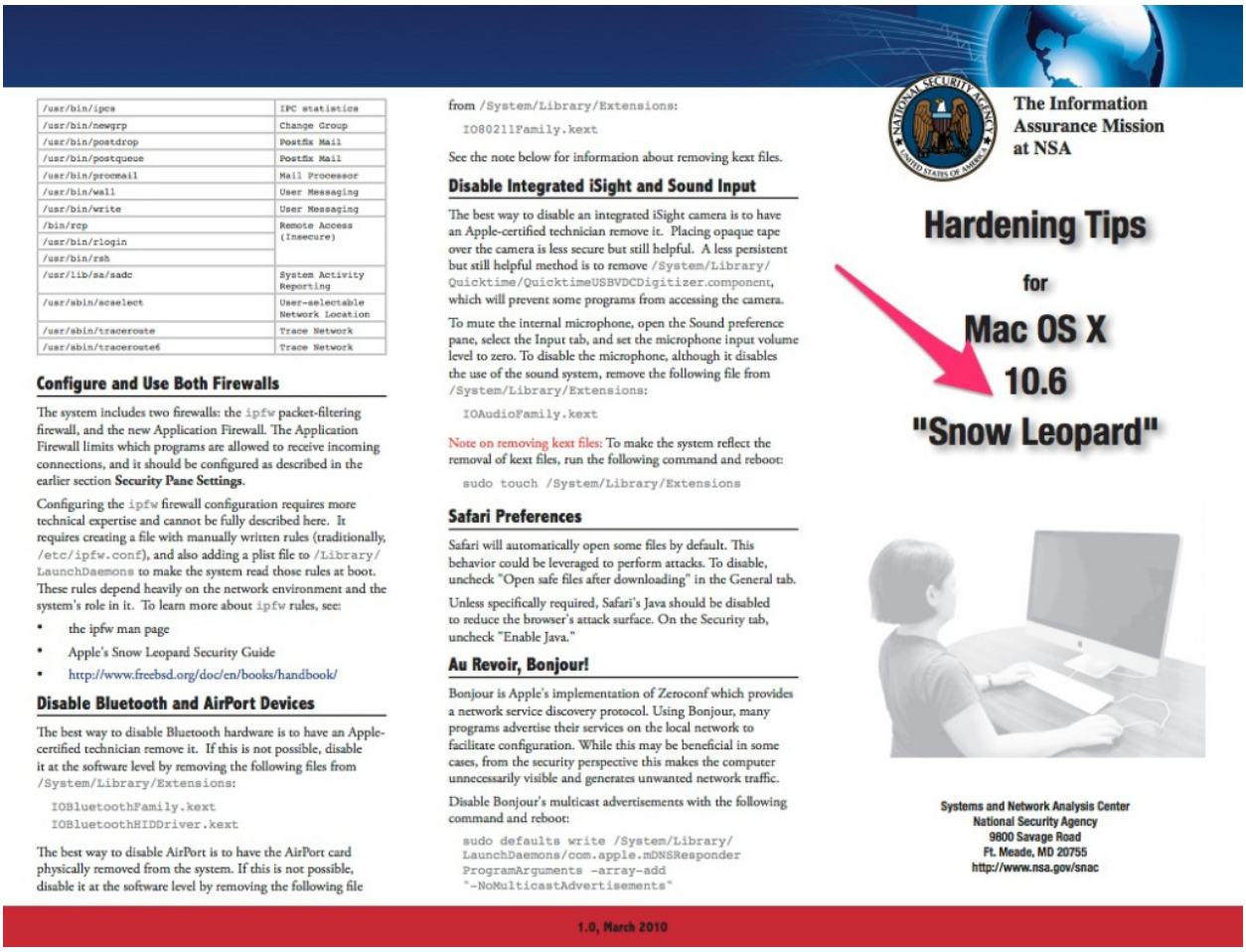
After identifying setuid and setgid binaries, disable setuid and setgid bits (using `chmod ug-s programname`) on those that are not needed for system or mission operations.

The following files should have their setuid or setgid bits disabled unless required. The programs can always have their setuid or setgid bits re-enabled later if necessary.

For more information see Apple's Snow Leopard Security Guide chapter 7.

Filename:	Needed For:
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent	Apple Remote Desktop
/System/Library/Printers/IOMs/LPRIOM.plugin/Contents/MacOS/LPRIOMHelper	Printing
/sbin/mount_nfs	NFS
/usr/bin/at	Job Scheduler
/usr/bin/atq	Job Scheduler
/usr/bin/atrm	Job Scheduler
/usr/bin/chpass	Change user info
/usr/bin/crontab	Job Scheduler

Figure 1



/usr/bin/ipcs	IPC statistics
/usr/bin/newgrp	Change Group
/usr/bin/postdrop	Postfix Mail
/usr/bin/postqueue	Postfix Mail
/usr/bin/procmail	Mail Processor
/usr/bin/wall	User Messaging
/usr/bin/write	User Messaging
/bin/rcp	Remote Access (Insecure)
/usr/bin/rlogin	
/usr/bin/rsh	
/usr/lib/sa/sadc	System Activity Reporting
/usr/sbin/scselect	User-selectable Network Location
/usr/sbin/traceroute	Trace Network
/usr/sbin/traceroute6	Trace Network

Figure 2

How you find a balance between security and convenience depends entirely on you. Clearly, the NSA needs to keep their computers as "hard" as possible. The trade-off for them is the loss of some functionality for their computers, but they end up with very secure computers from the process. A balance for security and convenience for home use is a computer sitting behind a router with a hardware "firewall", a software "firewall" activated on the computer, updated and patched software, safe password and internet surfing habits. For those of you that feel the need for more security (and less concern about convenience), the number of processes and settings on the following pages will be helpful.

Finally, I could not find any more current documents available from the NSA on hardening Mac OS X. As mentioned earlier, the info at hand will be for OS X 10.6, we are using 10.9, with the introduction of 10.10 just around the corner. As a result, not everything mentioned here will work on current versions of OS X. Where changes exist, to the extent of my knowledge, they will be discussed. Before you continue, a word of caution: Don't attempt something that does not make sense to you, or you feel is beyond the scope of your skill sets. I once had a Linux distribution on one of my desktop computers so secure that I couldn't log into it. It took me hours to diagnose and undo the damage I had done. Please don't follow my example.

Don't Surf or Read Mail Using an Admin Account

For 10.7 and up, go to System Preferences > Users & Groups. Click on the Padlock icon in the lower left corner of the window, to "unlock" the window. Click the "+" button in the lower left corner of the sidebar to add a new User. Be sure not to grant this account Administrator privileges. This should be your daily "go to" account, using only the Admin account to do system wide processes and settings. On the left side of the window click on the new User; in the right side of the window, click the Change Password button, and follow the instructions. The password should be unique, and not used anywhere else (if you use the same password in several locations, like your computer, access to your bank account on the internet, Netflix, etc., a Bad Guy that obtains your password now has access to all the places we have just mentioned). The password should be 10 or 12 digits, and have both upper and lower case letters, numbers, and punctuation. Your new user account will make getting your Mail and using the web safer as installing malware, trojans, etc., are now much more difficult for bad guys to carry out. While you are at it, you might want to reset passwords for each of your users, using the process for developing safer passwords. Be sure to click the Padlock in the lower left hand corner of the window when you are done, to lock in your changes.

As we now have passwords for many places of access, you should consider using a password manager. Most password managers encrypt your passwords, store them, and automatically insert them, as needed. In addition, they can also generate new passwords for you. I use the free version of LastPass. (For more information about LastPass, click here)

Use Software Update

Note: To make changes in the *System Preferences* panes, be sure to unlock the Padlock icon in the lower left corner of the window by clicking on it, and supplying a password when prompted. When you have completed your changes re-lock the Padlock icon by clicking on it again.

For 10.6, NSA's instructions are still good.

In 10.7, go to *System Preferences > Software Update*. Be sure these boxes are checked:

Check for updates: Weekly
Download updates automatically

On 10.8 and 10.9, go to System Preferences > App Store and be sure these boxes are checked"

Automatically check for updates
Download newly available updates in background
Install app updates
Install system data files and security updates

Account Settings

In 10.7, *Account Settings* was renamed *Users & Groups*. From *System Preferences*, open *Users & Groups*. Click the Padlock icon in the lower left hand corner, and give the proper password when prompted. Now, set *Automatic Login* to *Off*, and then set Display login window as *Name and Password*. From now on, when you login, no reference to the last "User" will be shown on the login screen. Next, uncheck the box *Show password hints*.

In the sidebar on the left of the window, click Guest User. Note that the right side of the window now displays setup information for the Guest account. Now uncheck:

Allow Guest to log into this computer
Allow Guest to connect to shared folders

Figure 3

Click on each user account in the left sidebar, and in the right part of the window, uncheck *Allow user to reset password using* Apple ID. With this item left checked, as in Figure 3, someone with your Apple ID could reset your password, and lock you out of your computer. Now, click the Padlock icon on the lower left corner of the window to lock it.

Security Settings

Figure 4

Since 10.6, this has changed a great deal. Go to *System Preferences* > *Security & Privacy*, and once again, unlock the Padlock icon on the lower left corner of the window.

In the General Tab:

- Check *Require password after sleep or screen saver begins*, and set the drop down box to *immediately*.
- Now, check *Disable automatic login*.
- Check Allow apps downloaded from: *Mac App Store and identified developers* (You can still install other downloaded applications by Command-clicking them and selecting open)
- As an option, click the *Advanced* button in the lower right hand corner of the window, and uncheck *Automatically update safe downloads list(*2).

The FileVault Tab

FileVault 2 is a good option for mobile devices, for a desktop computer it maybe a bit of over-the-top. To enable it, click *Turn on FileVault*, and follow the instructions. During the process you will be supplied a recovery key. If you forget your password, this will be your only way to use your Mac Click the *Turn On Firewall* button.

- Click the *Firewall Options* button.
- Be sure *Automatically allow signed software to receive incoming connections* is checked
- Turn on *Enable stealth* mode.

The Privacy Tab

- Be sure *Location and Services* is highlighted in the left sidebar, and above the right portion of the window, uncheck *Enable Location Services*.
- Click *Diagnostics & Usage* and uncheck *Send diagnostic and usage data to Apple*.
- Click the Padlock in the lower left and corner of the window to its locked state.

Home Folder Permissions

From the original document:
To prevent users and guests from perusing other users' home folders, run the following command for each home folder(3):

sudo chmod go-rx /Users/username

Firmware Password

NSA's instructions here no longer work. Boot into the *Recovery* partition by pressing Command-R, while the Mac is booting. Then select *Utilities>Firmware>Password Utility* and set the password. You will need it when you boot into a recovery mode or from an external drive(4).

Disable IPv6 and Airport When Not Needed

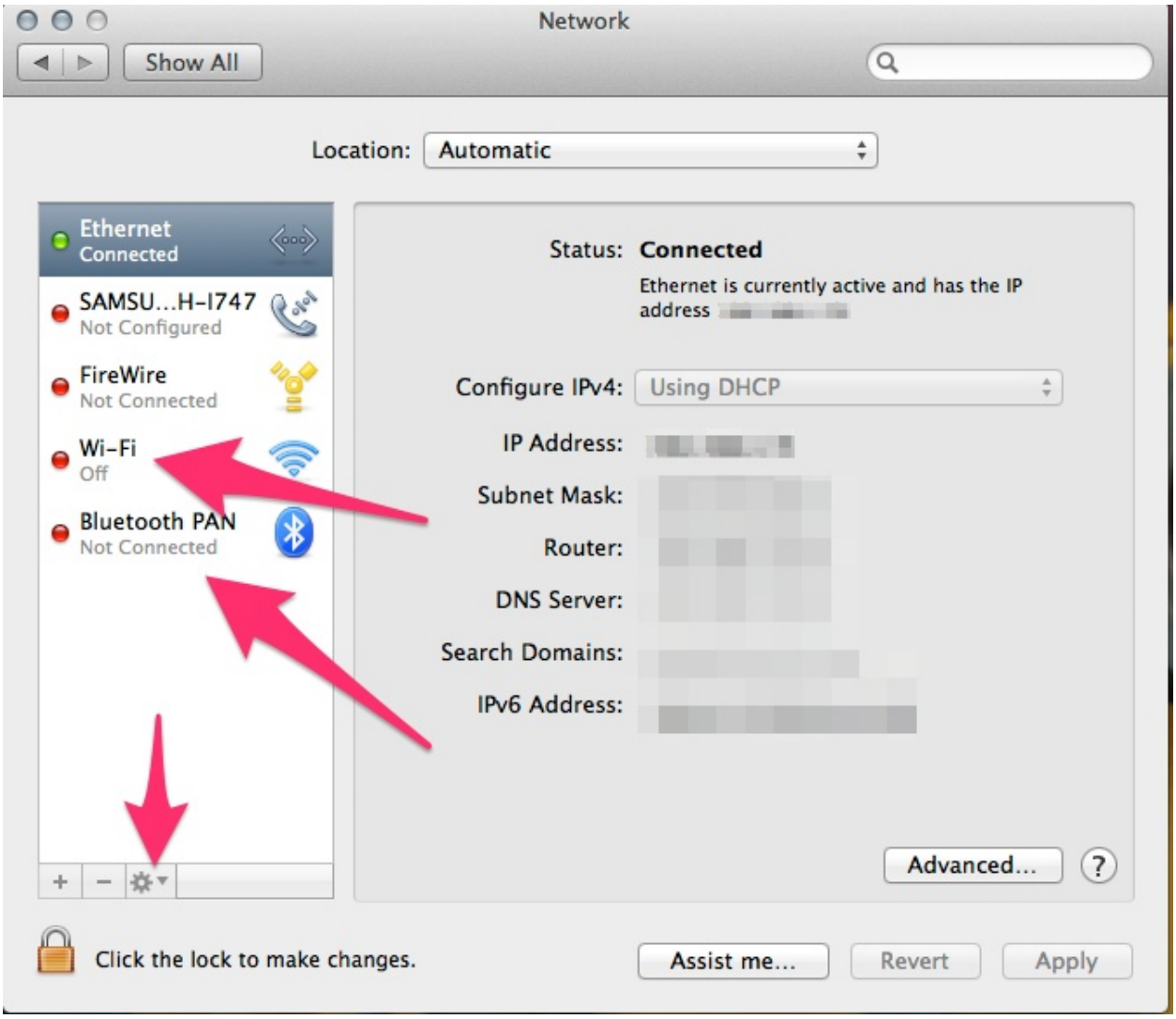


Figure 5

Disable Airport

- Go to *System Preferences* > *Network*
- Unlock the window (Padlock)
- Click *Wi-Fi* in the sidebar
- Click the Gear icon in the bottom part of the sidebar
- Select *Make Service Inactive*

Disable IPv6

- On the lower right side of the window, click the *Advanced* button.
- Set the drop down box next to *Configure IPv6 to Link-local only*.
- Lock the Padlock

Unnecessary Services

Disabling unnecessary services affects your computer by limiting some functionalities. I can see where being slightly paranoid about unneeded services is logical for a security branch

of the government, but for us mortals, it is best to follow the adage: “if it ain’t broke, don’t fix it”.

Disable Setuid and Setgid Binaries
Unless you really really really know what you are doing (in which case you probably aren’t reading this), do not disable any of these binaries. There are far more inherent risks in doing this than there are benefits.

Disable Bluetooth and Airport Devices
We already disabled Wi-Fi (Airport) above, in *System Preferences* > *Network*. Disable Bluetooth the same way.

Safari
Open Safari, then go to Safari > Preferences > General and uncheck Open safe files after downloading. Now leave the General tab, and go to the Security tab, and uncheck Enable Java.

To surf the net more safely you might consider an anonymous proxy, either web-based, direct, or software based. The Tor network is an example of an anonymous proxy. You can find out more about anonymous proxies here.

Au Revoir, Bonjour!
Using Bonjour, many programs advertise their services on the local network to ease configuration. While this may be beneficial in some cases, from the security perspective this makes the computer unnecessarily visible and generates unwanted network traffic. Disable Bonjour’s multicast advertisements with the following command and reboot:

Sudo defaults write /System/Library/LaunchDaemons/
com.apple.mDSNResponderProgramArguments -array-add “- NoMulticastAdvertisements”

———————————————–
Article based on information from Hardening Tips for Max OS X 10.6, Snow Leopard
http://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf