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

/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

Configure and Use Both Firewalls

The system includes two firewalls: the `ipfw` packet-filtering firewall, and the new Application Firewall. The Application Firewall limits which programs are allowed to receive incoming connections, and it should be configured as described in the earlier section **Security Pane Settings**.

Configuring the `ipfw` firewall configuration requires more technical expertise and cannot be fully described here. It requires creating a file with manually written rules (traditionally, `/etc/ipfw.conf`), and also adding a plist file to `/Library/LaunchDaemons` to make the system read those rules at boot. These rules depend heavily on the network environment and the system's role in it. To learn more about `ipfw` rules, see:

- the ipfw man page
- Apple's Snow Leopard Security Guide
- http://www.freebsd.org/doc/en/books/handbook/

Disable Bluetooth and AirPort Devices

The best way to disable Bluetooth hardware is to have an Apple-certified technician remove it. If this is not possible, disable it at the software level by removing the following files from `/System/Library/Extensions`:

```
IOBluetoothFamily.kext
IOBluetoothHIDDriver.kext
```

The best way to disable AirPort is to have the AirPort card physically removed from the system. If this is not possible, disable it at the software level by removing the following file from `/System/Library/Extensions`:

```
IO80211Family.kext
```

See the note below for information about removing kext files.

Disable Integrated iSight and Sound Input

The best way to disable an integrated iSight camera is to have an Apple-certified technician remove it. Placing opaque tape over the camera is less secure but still helpful. A less persistent but still helpful method is to remove `/System/Library/Quicktime/QuicktimeUSBVDCDigitizer.component`, which will prevent some programs from accessing the camera.

To mute the internal microphone, open the Sound preference pane, select the Input tab, and set the microphone input volume level to zero. To disable the microphone, although it disables the use of the sound system, remove the following file from `/System/Library/Extensions`:

```
IOAudioFamily.kext
```

Note on removing kext files: To make the system reflect the removal of kext files, run the following command and reboot:

```
sudo touch /System/Library/Extensions
```

Safari Preferences

Safari will automatically open some files by default. This behavior could be leveraged to perform attacks. To disable, uncheck "Open safe files after downloading" in the General tab.

Unless specifically required, Safari's Java should be disabled to reduce the browser's attack surface. On the Security tab, uncheck "Enable Java."

Au Revoir, Bonjour!

Bonjour is Apple's implementation of Zeroconf which provides a network service discovery protocol. Using Bonjour, many programs advertise their services on the local network to facilitate 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.mDNSResponder
ProgramArguments -array-add
"-NoMulticastAdvertisements"
```

The Information Assurance Mission at NSA

Hardening Tips

for

Mac OS X 10.6 "Snow Leopard"

Systems and Network Analysis Center
National Security Agency
9800 Savage Road
Ft. Meade, MD 20755
http://www.nsa.gov/snac