The following tips assume that the reader is starting with a default installation of Mac OS X 10.5 (Leopard). These tips may not translate gracefully for previous versions.

Important: System updates may override many of these configuration changes. Achieve their persistance using a script and a cron job or vigilant re-application.

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 "Disabled." Set login window to display as "Name and password."

Disable guest account and sharing: Select the Guest Account and then disable it by unchecking "Allow Guest to log into this computer." If this feature must be used, deselect "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 to wake this computer from sleep or screen saver
- Disable automatic login
- Use secure virtual memory
- Disable remote control infrared receiver (if present)

In the FileVault tab, read the warnings and consider activating FileVault. FileVault is most appropriate for portable systems, since it can protect their data even if the system itself is stolen.

In the Firewall tab, select "Allow only essential services." Next, click on the "Advanced..." button and enable the "Firewall Logging" and "Stealth Mode" options.

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
```

Physical Security

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

For PowerPC-based Systems:
Access the Open Firmware command interface by holding down ⌘-Option-O-F during startup. At the prompt, type `password` to set a password. Inexplicably, a capital "U" cannot be used in the password. Next, select a security level and set it with the following command:

```
setenv security-mode securitymode
```

`none` is the default and will not prompt the user for a password, `command` will prompt the user for a password when they attempt to make changes to Open Firmware settings, and `full` will additionally prompt the user for a password every time they boot the system. `command` is recommended.

For Intel-based Systems:
To change the firmware password, use the Firmware Password Utility. It can be found on the Leopard Install DVD in the hidden folder `/Applications/Utilities`, accessible from the Go menu's "Go to Folder..." option in the Finder or in the menu bar during installation. The password you choose will be the password required to change firmware settings or boot off external media.

Turn off 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 from wireless networks 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 PathToPlistFile
```

Filename:	Needed for:
com.apple.mDNSResponder.plist	Bonjour
com.apple.mDNSResponderHelper.plist	Bonjour
com.apple.dashboard.advisory.fetch.plist	Dashboard Auto-Update
com.apple.UserNotificationCenter.plist	User notifications
com.apple.RemoteDesktop.PrivilegeProxy.plist	ARD
com.apple.IIDCAssistant.plist	iSight
com.apple.blued.plist	Bluetooth

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
```

The following files should have their setuid or setgid bits disabled (using `chmod ug-s programname`) unless required for the purpose listed in the second column. The programs can always have their setuid or setgid bits re-enabled if necessary for the purpose shown.

Filename:	Needed For:
/Applications/System Preferences.app/Contents/Resources/installAssistant	Nothing
/Applications/Utilities/ODBC Administrator.app/Contents/Resources/iodbcadmintool	ODBC Administration

/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent	Apple Remote Desktop
/System/Library/Extensions/webdav_fs.kext/Contents/Resources/load_webdav	WebDAV Web Services
/System/Library/Filesystems/AppleShare/afpLoad	Apple File Protocol Sharing
/System/Library/Filesystems/AppleShare/check_afp.app/Contents/MacOS/check_afp	Apple File Protocol Sharing
/System/Library/Frameworks/ApplicationServices.framework/Versions/A/Frameworks/PrintCore.framework/Versions/A/Resources/PrinterSharingTool	Printer Sharing
/System/Library/CoreServices/Expansion Slot Utility.app/Contents/Resources/PCIELaneConfigTool	Expansion Slot Utility
/System/Library/PrivateFrameworks/DesktopServicesPriv.framework/Versions/A/Resources/Locum	Privileged Finder File Operations
/System/Library/Printers/Libraries/aehelper	Printer Configuration
/System/Library/Printers/Libraries/csregprinter	Printer Configuration
/System/Library/PrivateFrameworks/DiskManagement.framework/Versions/A/Resources/DiskManagementTool	Disk Utility
/usr/libexec/dumpemacs	Nothing
/usr/libexec/xgrid/IdleTool	XGrid
/usr/sbin/vpnd	Hosting VPN Services
/sbin/mount_nfs	NFS
/sbin/route	Network Config
/usr/bin/lppasswd	Printer Sharing
/usr/bin/ipcs	IPC statistics
/bin/rcp	Remote Access (Insecure)
/usr/bin/rlogin	
/usr/bin/rsh	
/usr/lib/sa/sadc	System Activity Reporting
/usr/sbin/pppd	PPP
/usr/sbin/scselect	User-selectable Network Location

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, consult the following resources:

- the `ipfw` man page
- IPFW section in FreeBSD manual (available online)

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, *even if it means crippling 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 Settings

In the Safari web browser, choose "Preferences..." from the "Safari" menu. In the General tab, de-select "Open safe files after downloading."

Hardening Tips

For Default Installation of

Mac OS X 10.5 "Leopard"

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