FOUNDATIONS OF MAC OS X LEOPARD SECURITY

ISBN-13 (pbk): 978-1-59059-989-1

ISBN-10 (pbk): 1-59059-989-6

ISBN-13 (electronic): 978-1-4302-0646-0

ISBN-10 (electronic): 1-4302-0646-2

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Lead Editor: Jeffrey Pepper
Technical Reviewers: Mike Lee, Frank Pohlmann
Editorial Board: Clay Andres, Steve Anglin, Ewan Buckingham, Tony Campbell, Gary Cornell, Jonathan Gennick, Matthew Moodie, Joseph Ottinger, Jeffrey Pepper, Frank Pohlmann, Ben Renow-Clarke, Dominic Shakeshaft, Matt Wade, Tom Welsh
Project Manager: Candace English
Copy Editor: Kim Wimpsett
Associate Production Director: Kari Brooks-Copony
Senior Production Editor: Laura Cheu
Compositor: Susan Glinert Stevens
Proofreader: Nancy Bell
Indexer: Julie Grady
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail orders-ny@springer-sbm.com, or visit http://www.springeronline.com.

For information on translations, please contact Apress directly at 2855 Telegraph Avenue, Suite 600, Berkeley, CA 94705. Phone 510-549-5930, fax 510-549-5939, e-mail info@apress.com, or visit http://www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at http://www.apress.com/info/bulksales.

CHAPTER 1

Security Quick-Start

If you are looking for a quick-and-dirty start to securing your Mac, this is the chapter for you. This chapter is meant as a quick-start, written for the "I need to get my Mac secured right away" readers. For the quick-and-dirty basics of getting your Mac secured, follow the instructions in this chapter. From Chapter 2 on, you'll be introduced to all the other intricacies surrounding securing the Mac OS, and we'll explain why we suggest the quick-start steps in more detail. Keep in mind that Chapter 1 gives just the basics, and although it will leave you with a fairly secure system, it's not as comprehensive as the subsequent chapters, where we delve deeper into the specifics of most settings. To get a more thorough understanding of Mac OS X security and the tools you can use to secure your Mac, we urge you to keep reading beyond the basics.

Securing the Mac OS X Defaults

Mac OS X, because it is built on a Unix architecture, is a fairly secure and stable operating system right out of the box. There is a commonly held belief that the Mac can be further secured only through the Unix command line and that the graphical user interface (GUI) does not need to be tinkered with to make it more secure. This could not be further from the truth. There are many ways in which Mac OS X can and should be made more secure without dipping into the Unix command line.

In fact, there are many security holes built into the Mac OS intentionally. Why is that? The answer lies in the relationship between ease of use and security. Generally, in the world of operating systems, the easier an operating system becomes to use, the less secure it is. When the engineers at Apple redesigned their OS from 9 to X, with the most advanced operating system architecture out there, they considered security very heavily, but they also considered usability. To ensure the most secure operating system possible without sacrificing ease of use, many security features are disabled by default, giving you, the user, the choice of whether to practice good security by enabling or disabling the features.

Having said that, many features of Mac OS X are already fairly secure without changing anything out of the box, with little—or no—trade-off to functionality. In fact, certain features should not be changed unless changing them is absolutely required; for example, you should not enable the root account unless you need to run a process that requires it, as is the case with programs such as Carbon Copy Cloner. Remember that when defaults are temporarily changed to complete certain tasks, you will need to go back and undo the changes after you have completed the tasks that required the change. Many security breaches occur because users forget to put security settings back the way they were.

Customizing System Preferences

The default settings for Mac OS X's System Preferences are fairly secure but can be further optimized to provide a higher level of protection. Seemingly innocuous settings can be used to exploit some of the Mac's core features. Therefore, to reduce the likelihood that this will occur, you should go through the options listed throughout the next few pages and disable any that aren't being used. You can then enable any security features that will not conflict with your needs along the way.

One of the most important concepts to understand with OS X security is that your computer is a multiuser operating system. Every machine has at least one user account and one local administrative account (sometimes referred to as the *root* account), which has access to take ownership of all the files on the system. There will always be more than one account on the machine and thus the potential for multiple breaches in security. In the next section, we will be getting a little more familiar with account settings and the ways in which you can secure users in the Accounts preference pane.

Accounts Preferences

In this section, we will tackle the most important topic: passwords. Your system is only as secure as your passwords. The stronger a password, the longer it will take to break. In Mac OS X, Apple has developed the Password Assistant to assist with password security. To set a password, open the Accounts preference pane, and click your account. This opens a window with your name, short name, and an option to change your password (see Figure 1-1). The name is typically your full name or the full name you may have entered when the account was created. The short name is a shortened version of the name (the first letter of the first word and the full second word by default).

■ **Note** We'll discuss users and groups in detail in Chapter 3. We will touch on a few of the important points in this section: disabling login items, setting account types, and basic user security.

Notice that there is no password; there is only an option to change a password. Apple carefully designed this pane so that a user could not easily view another user's password; with administrator access, they would only be able to change it. This is becoming a fairly standard practice with password handling industry-wide. When you click the Change Password button on the Accounts preference pane, a smaller window will pop up asking you to type the old password and then the new password (see Figure 1-2). You must enter the new password twice to ensure accuracy.

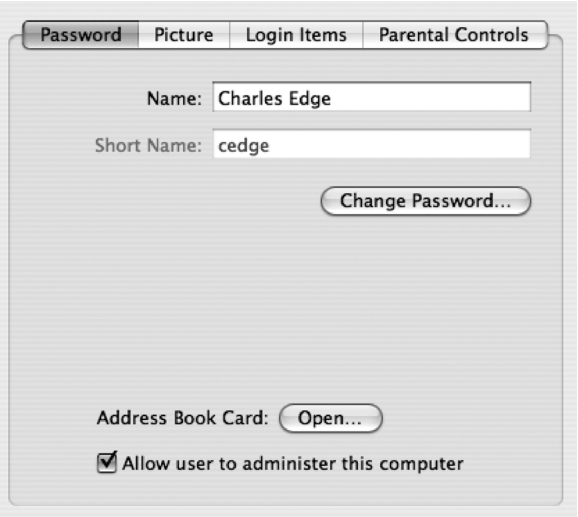

Figure 1-1. *Account settings*

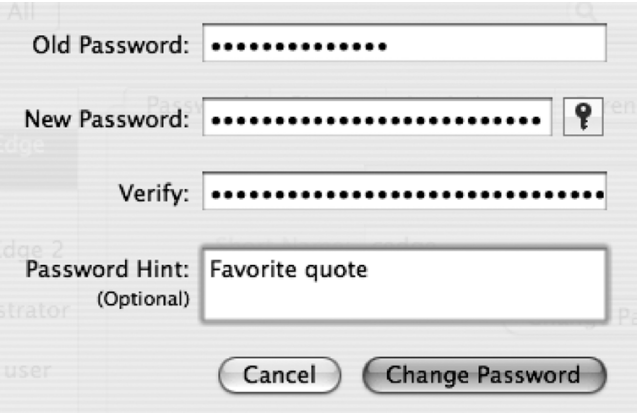

Figure 1-2. *Changing a password*

Clicking the key icon in the Change Password window opens the Password Assistant (see Figure 1-3). The Password Assistant is a random password generator that can be used to help create a more secure password. It's a great utility if you need suggestions for more complex passwords. All too often users will use passwords such as *password* and *god*. This tool was created to counteract this alarming trend.

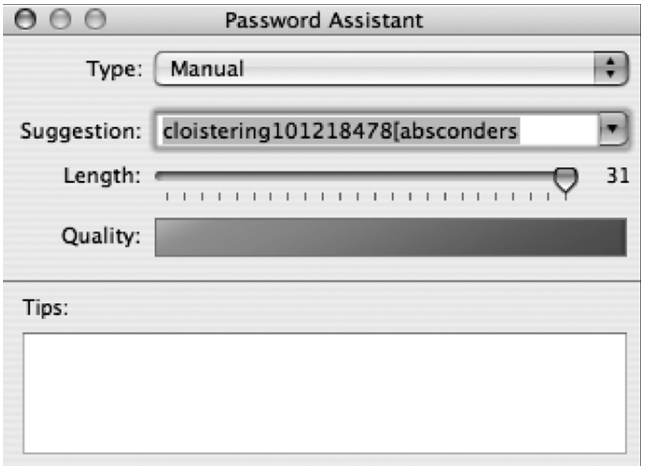

Figure 1-3. *Password Assistant*

■ **Note** When setting passwords, you should include numbers, letters, and special characters, such as !, @, #, or $. Using various sets of characters yields very secure passwords.

Login Options

To make the login screen more secure, you should alter the default settings of the Login Options tab in the Accounts preference pane. Click the Login Options button of the Accounts preference pane. (You may need to click the little padlock icon at the bottom of the screen to access this screen as an administrator.) The Show the Restart, Sleep, and Shut Down Buttons option of the Login Options window (see Figure 1-4) is enabled by default. If this option is disabled, when the machine boots, it will hide these buttons at the login window so that users cannot shut the system down at the login screen. Any systems that provide services that need to be running for other users should have this option disabled.

The Show Password Hints option can be helpful if you need a hint to remind you of your password in case you forget it. However, this can also give someone trying to guess your password valuable insight into what the password may be. For example, it is common to have a hint something along the lines of "My dog's name." This would require very little effort on the part of someone attempting to break into your system to guess your password. All too often, we find that users enter the actual password into the password hint field. Obviously, this is not best practice in any situation unless it is merely impossible for you to memorize your password.

■ **Tip** If you do need help remembering your password, using password hints are better than writing passwords down.

Figure 1-4. *Login options*

The Enable Fast User Switching option is a way to allow multiple users to log into the computer concurrently. This allows users to stay logged in while accessing other accounts. It poses a security risk, though, because it is possible to access or alter processes being run by other users. To limit what each user can do to access another user's processes, make sure that all nonadministrative users are not allowed administrative access to the system. Better yet, if this is a feature that you are not likely to use, disable it by unchecking the Enable Fast User Switching option. If you do enable it, you will see the message in Figure 1-5 warning you that this is a security risk.

Figure 1-5. *Fast user switching warning*

The administrative user should be logged in only when administrative tasks (changing passwords, configuring network settings, and so on) are necessary, not for everyday work. This is a key component of Unix system administration and a good way to keep from harming the system by accident or accidentally allowing a rogue process to harm the system. Running a

second account also gives you a path to get into the computer should something render your regular, nonadministrative login account inoperable.

To create a second account to use, open System Preferences, and go to the Accounts preference pane. From here, click the lock to unlock the preference, and click the + symbol to add the account (see Figure 1-6). Leave the type set to User Account, and enter the name, short name, and password you want the account to have. Do not check the Allow User to Administer This Computer box if this is the nonadministrative account for regular use of your system. Now click Create Account.

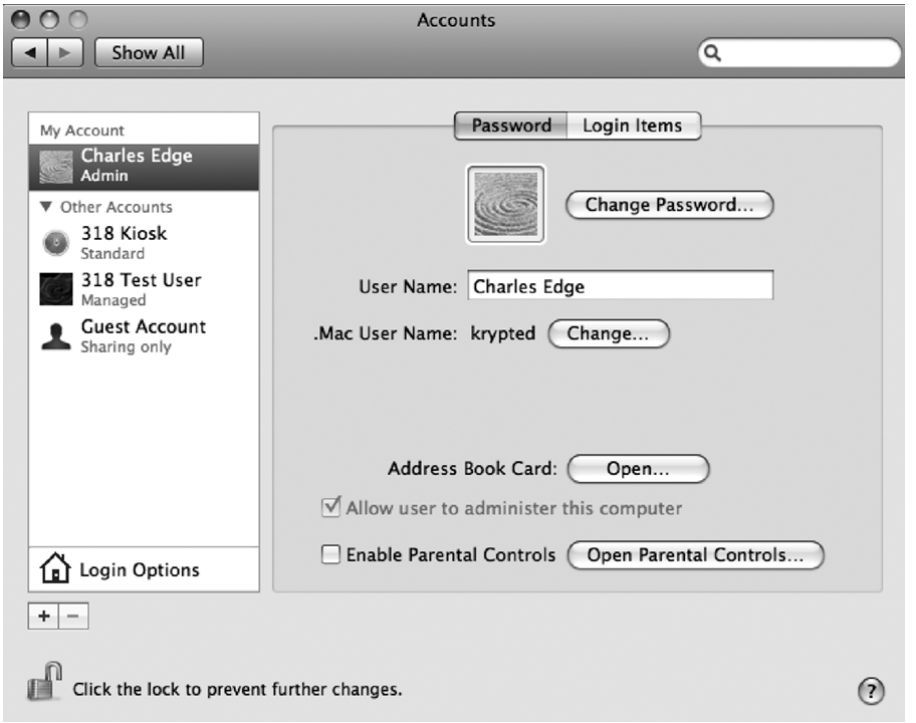

Figure 1-6. *Creating an account*

Once you have created the new account, log out of the administrative account and log in as your nonadministrative account. Remember, you can always copy your documents, music, and other data out of your administrative account and, if need be, log in as the administrative user to access anything that won't copy using the regular user. Migrating your user profile to a nonadministrative user creates a much more secure computing environment.

Security Preferences

Another place to change the default settings for security purposes is in the Security preference panel (see Figure 1-7). Here, you will find options (that we explain in the rest of this section) for enabling many of the miscellaneous security features that Apple has developed that do not fit into any other System Preferences panel. There are other items that allow for heightened security, but these are typically located within the applications or operating system features they were

designed to protect. Some of these basic security features we will review later in this chapter. Others will be reviewed throughout the remainder of the book.

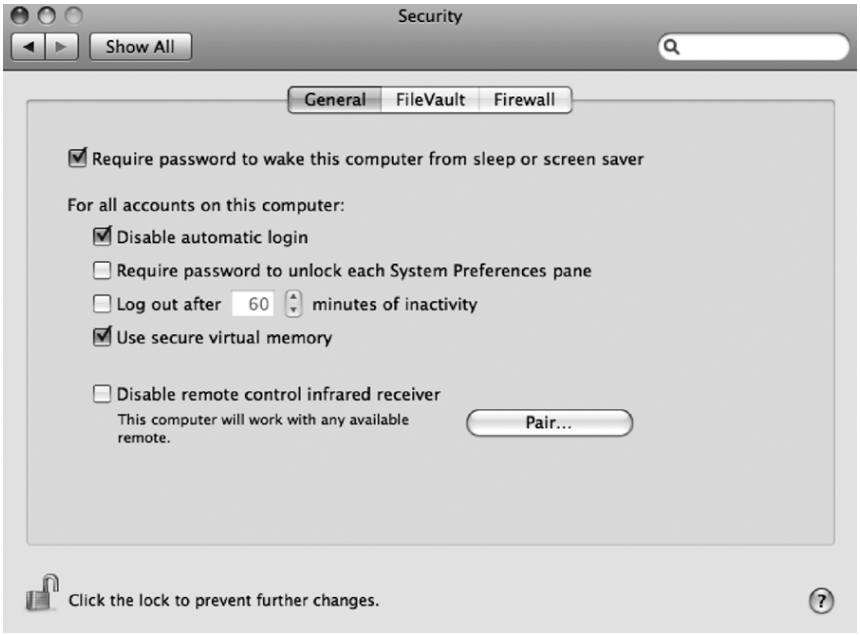

Figure 1-7. *Security preference pane, General tab*

The first and most important of these options is the automatic login, which allows anyone with physical access to your computer to restart the computer and, if the password is remembered, not be required to enter a password in order to get your data. Automatic login is enabled by default. This is one of the first things you should change because it gives people the ability to log into your system and access your data. With automatic login enabled, few of the other options to secure your computer are relevant because they already have access to your computer.

You can use the option called Require Password to Wake This Computer from Sleep or Screen Saver on the General tab of the Security preference pane to force your computer to require a password to wake it up after it has gone to sleep or after the screen saver has been activated. This is critical and is not enabled by default. The Require Password to Wake This Computer from Sleep option makes it easy to lock your system, whether in a timed or manual way. Using the Exposé application to assign a key or *hot corner* (moving the cursor to a corner of the screen to activate the display) to put a system to sleep allows you to put your machine to sleep when you are finished using it. Later in this chapter we will review setting up automatic sleep, Exposé, and screen saver options.

The option Logout When Inactive allows users to have their systems logged out whenever they are left inactive for a period of time. This setting supersedes any settings for putting a system to sleep or activating a screen saver. The automatic logoff option will log users out of their accounts when they are inactive. This can be a dangerous feature because it is possible for users to lose data they were working on if the machine automatically logs them out.

Virtual memory is a means of using hard drive space as temporary memory in order to allow the computer to perform more work than the computer has available memory for. Virtual memory creates virtual chunks of memory in files called *swap files* on your hard drive. When this transitory memory is no longer needed, the swap files are deleted (which doesn't always happen immediately). Valuable information can be gleaned from a system by viewing the virtual memory swap files and reconstructing user operations. The option to secure virtual memory encrypts the swap files, preventing others from using them to gather private data. This is an important feature to enable.

FileVault

Let's face it. We're human, and we forget passwords all the time. What happens when you forget the password for your computer and you are the only one with an account on the machine? On the Web, there is a system that web sites use when users forget their passwords. It's called a *self-service password reset* whereby they can reset the password on their own (usually by answering a secret question on a web prompt and then receiving a new temporary password via e-mail). For a machine with many users, this would certainly be a handy feature to have and would significantly reduce the volume of calls to the help desk. Apple supplied Mac owners with this feature via the password reset utility included on the Mac OS X CD. You can boot a computer to the CD and reset the password at any time by rebooting the computer and holding down the C key.

But what if you want to limit someone's ability to access your data if they were able to reset the password? Many of us travel with laptops that, if stolen and the password were to be reset, would give users access to data they shouldn't be able to access. For example, students would have access to tests, children would have access to our web site viewing habits, employees would have access to confidential data about other employees—all if they were able to get physical access to our computers while we were away. The ability to easily reset a password introduces you to a feature of the Mac OS X security preferences that protects data, even if the password is reset using the CD: FileVault. FileVault removes the ability to access data in a user's folder, even if the password is reset, by encrypting the contents of a user's home folder into a secured disk image.

■ **Note** The FileVault feature is only as strong as the password protecting the home folder.

FileVault is not for everyone. It can cause some inconveniences. By enabling FileVault, Windows file sharing and printer sharing are disabled. By enabling FileVault, you will break these connections if another user is relying on them, so be cautious. It will sometimes slow down the logout process because it encrypts the data in the logout process. FileVault can also have complications with certain applications, such as Adobe Illustrator. If you suspect that FileVault is causing an application to be problematic, then turn it off to see whether that fixes the issue. Even with these inconveniences, FileVault is an excellent way to secure the data on your machine.

To use FileVault, you will need to set it up in the Security preference pane. Open System Preferences, and click Security (see Figure 1-8). Then click the FileVault tab. Next, click Turn On FileVault. At this point, you will need to give the system a master password. The master password can unlock any FileVault on a computer, so it needs to be a strong one. To enable the master password, click the Set Master Password button, and type the password you want to use twice. Then, enter a hint to help you if you forget it at a later date (do not enter the password itself!), as shown in Figure 1-9.

Figure 1-8. *Setting up FileVault*

Note If you suspect that others will enable FileVault to encrypt their home folders, such as students, children, or employees, then setting up a master password before they can enable FileVault will help ensure that you will always be able to log into any FileVault disk images that are created by other users on the system.

At this point, you will be prompted for the password of the account you are currently logged into. You can stop the process of encrypting the user's home folder and just enable a master password by clicking Cancel (see Figure 1-10), or you can encrypt the user's home folder by entering the password for the user and clicking OK. Keep in mind that the amount of time the encryption takes depends on how large the home folder is. It can take a while, so be patient. Interrupting the process can cause corruption or cause you to have to start the process all over again.

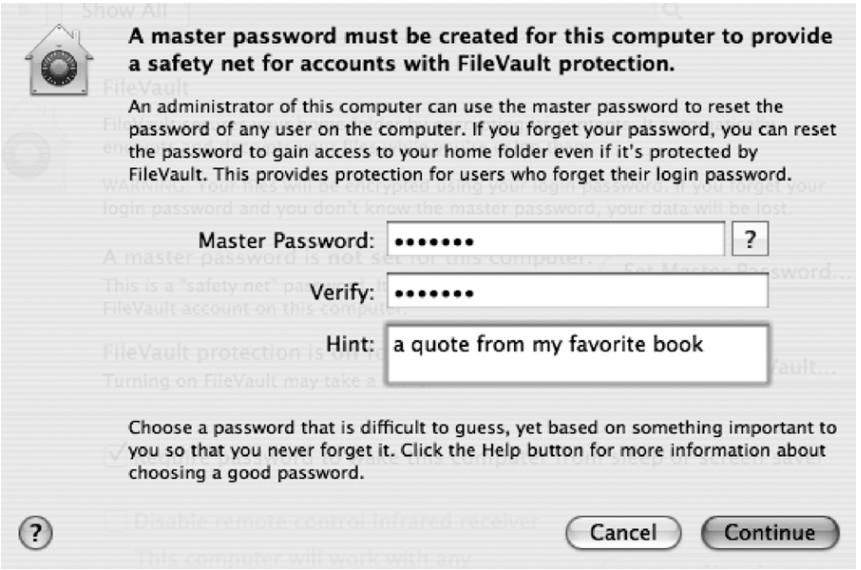

Figure 1-9. *Setting the master password*

Figure 1-10. *Authenticating to an account*

If you want to change FileVault settings later, you can do so by returning to the Security preference pane (see Figure 1-10). You can change the master FileVault password or turn off FileVault completely (if the home folder is large, be prepared to wait a while for it to decrypt).

Infrared Controls in Security Preferences

Apple is now shipping infrared remote controls with many of its new computers, including MacBooks, MacBook Pros, and iMacs. As of this book's publication, there is little that can be done to damage systems with the infrared remote controls; however, theoretically it does allow

someone to walk by the machine and launch menu options by use of a remote, which can be rather annoying. (If you do not have an infrared receiver, then you will not have this option in your Security Preferences.) Once the technology is more thoroughly utilized, there is also the theoretical chance that it could be used to exploit the system. This is a new concern since the release of the wifi exploit at DefCon 2006 by David Maynor that we cover further in Chapter 9.

Noticing this as a possibility, Apple introduced the ability to enable and disable the remote control infrared receiver in the Security preferences. If you still want to use an infrared receiver, you can pair the receiver to your system, which disables all receivers other than the one used to pair with the computer. To pair your infrared remote control with your computer, hold the fast-forward and menu buttons down on the remote for five seconds. If you will not be using an infrared receiver, then you should disable the ability to do so. To turn off the ability to use an infrared receiver, click the Security pane in System Preferences, and select Disable Remote Control Infrared Receiver (see Figure 1-11). You may also want to unpair the remote (because you have a new remote or lost your old one). To do this, simply click on the Unpair button in this window (Pair turns into Unpair when the remote is paired with the machine).

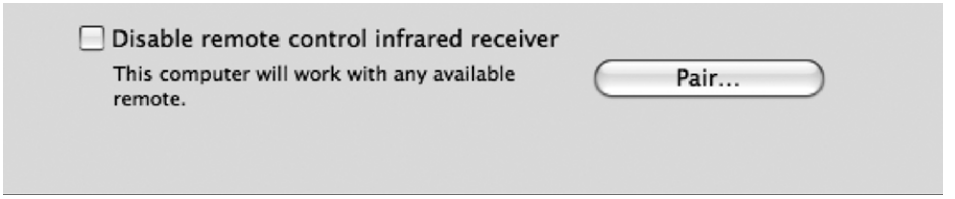

Figure 1-11. *Disabling the remote control infrared receiver*

Other System Preferences

The security features built into the Network preference pane include the ability to configure your client system to work with a proxy server and other advanced networking features. These advanced networking techniques will be covered in depth in subsequent chapters. Suffice it to say that networking options are aplenty here.

The Mac OS X firewall is a software-based application firewall built into the operating system designed to block unwanted network traffic. It is disabled by default, and you should usually enable it. To do this, open the Security preference pane, and click the Firewall tab. Then, select the Allow Only Essential Services option (see Figure 1-12).

■ **Note** We discuss the firewall in further detail in Chapter 8.

Figure 1-12. *Firewall options in the Security preference pane*

Software Update

You can use the Software Update preference pane to keep your system updated with the latest Apple updates and security patches (see Figure 1-13).

By default the Software Update feature is turned on, which means that the system will automatically search for updates on a weekly basis. There are rare situations where you will not want to run certain software updates because they can cause conflicts with other installed software, as has been the case with Apple QuickTime updates and the Final Cut software on multiple occasions. But for most users Software Update is one of the best ways to keep the latest and greatest security patches on their system, so it should be enabled. Before running any software updates on mission-critical systems, you should test them in a lab environment. Typically, security updates will not cause issues with other applications, but it is still wise to test them in a lab environment before installing them on mission-critical machines.

■ **Note** To manually run the Software Update feature, open the Software Update preference pane, and then click the Check Now button on the Update Software tab.

Figure 1-13. *Software Update preference pane*

For many, using the Mac OS X Software Update preference pane will be adequate to keep their computer updated. However, if you have multiple systems on your network that need updating, you can quickly bottleneck your Internet pipe if multiple users are downloading updates all at the same time. You will most likely want to deploy a solution to help you conserve your bandwidth by managing these updates. The Software Update Server feature in Mac OS X Server is a great solution for controlling Apple software updates. However, this is not going to be the right solution for everyone because it requires an OS X Server to use.

■ **Note** There are ways to run the Software Update Server feature without having it run on a Mac, but it is best to run it on Mac OS X Server for simplicity's sake.

Security updates should always be taken seriously and run when possible (see Figure 1-14). One unique aspect of the Apple Software Update preference pane is that security updates are always deployed independently from other updates. Security updates rarely force a restart of the computer and almost invariably contain a comprehensive description explaining what they fix and why they were written.

Occasionally a software update will fail. When this occurs, it is possible for the update to become stuck in the software update cache. To clear these out or retrieve them, browse to the `/Library/Caches/com.apple.softwareupdate/swcdn.apple.com` folder, and find the update on your system. The update will be located in the folder with the corresponding month and date (see Figure 1-15). You can delete the update or run it again from this location. If the update is not located in these folders, then you should be able to run the Software Update feature and have it install again after a restart. You can also utilize this technique to save the update and burn it to optical media or a network drive for future installations.

Figure 1-14. *List of security updates in Software Update*

Figure 1-15. *Navigating to where security updates are stored*

Bluetooth Security

Bluetooth is a globally unlicensed short-range radio frequency for wireless networks, also known as IEEE 802.15.1. In other words, Bluetooth is a wireless technology that provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), mobile

phones, laptops, PCs, printers, and digital cameras. The Apple Bluetooth keyboard and mouse are popular Bluetooth devices in Apple environments.

Bluetooth works by pairing two devices. Once two devices are paired, they are able to freely exchange data while paired. To pair a device with an Apple computer, you will need your computer to be *discoverable*, or awaiting a pairing. You are also required to accept the pairing in most cases. However, there are a variety of attacks that can force a pairing if your system is set to be discoverable without using a password. This creates a security vulnerability that can be prevented by not having Bluetooth enabled unless you are actively using a device via Bluetooth.

Bluetooth is enabled and discoverable by default. If you do not want to use Bluetooth on your system, then open System Preferences and select the Bluetooth preference pane. Once you have this pane open, then click the Turn Bluetooth Off button to disable Bluetooth on your system (see Figure 1-16). If you want to use Bluetooth but do not want your system to be discoverable, then you can disable discoverability by unchecking the Discoverable box on this pane.

Figure 1-16. *Bluetooth preference pane*

The Devices tab of the Bluetooth preference pane offers a way to view devices that have been paired with Mac OS X computers (see Figure 1-17). Here, you will see any devices previously paired and be able to configure each device with its appropriate settings.

The Sharing tab of the Bluetooth preference pane allows more granularity when configuring exactly what options are available for various types of Bluetooth connectivity (see Figure 1-18). Here, it's possible to allow for file transfer, file exchange, and synchronization between the device and the computer. If you are not using these features, then disable them because this is a prime target for attacks.

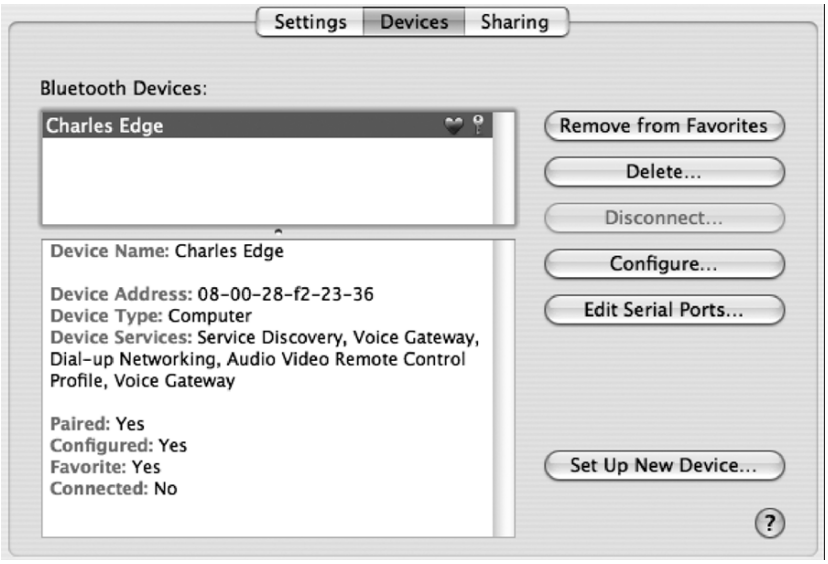

Figure 1-17. *Configuring Bluetooth devices*

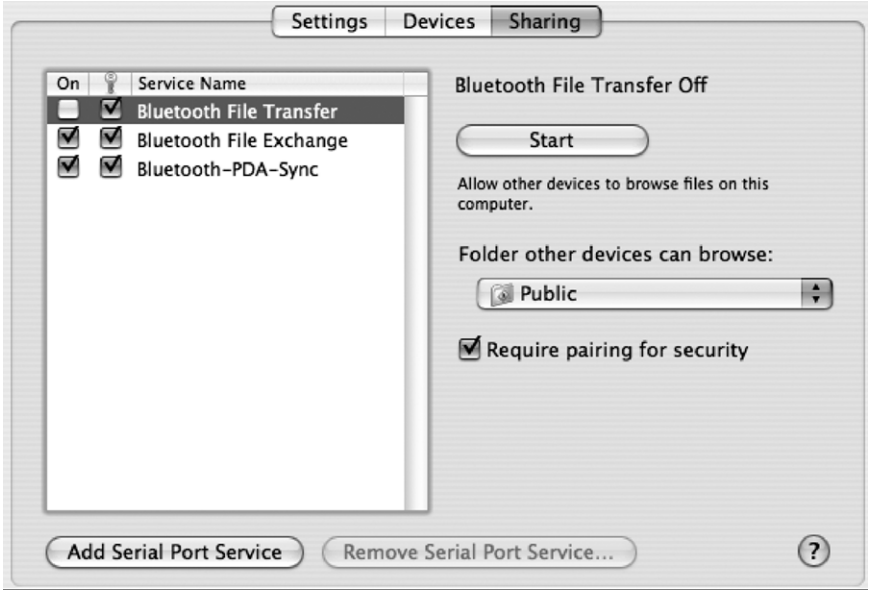

Figure 1-18. *Bluetooth sharing*

Bluetooth-PDA-Sync allows administrators to perform PDA synchronization using Bluetooth. Serial ports are often used to synchronize Palm Pilots, Blackberrys, and other devices. Bluetooth can operate as a wireless serial port. Here, it is possible to disable the Bluetooth-PDA-Sync feature by clicking the Edit Serial Ports button and clicking the Stop Serial Port button on the Edit Serial Port screen. If you do want to use Bluetooth as a serial port, you should leave the

Require Pairing for Security box checked because this will force a more secure pairing of the device.

Printer Security

In the move from Tiger to Leopard, Apple removed the Printer Setup utility. All controls for printing have now been moved into the Print & Fax preference pane in System Preferences. The Print & Fax preference pane offers few options for configuring access to shared printers and faxes. When sharing printers, only the printers that the user needs should be configured. Allowing a user to print to a printer that they shouldn't be using can cause confidentiality issues if the documents they are printing land in the wrong hands. To disable printers not in use, uncheck each printer on the Sharing tab (see Figure 1-19).

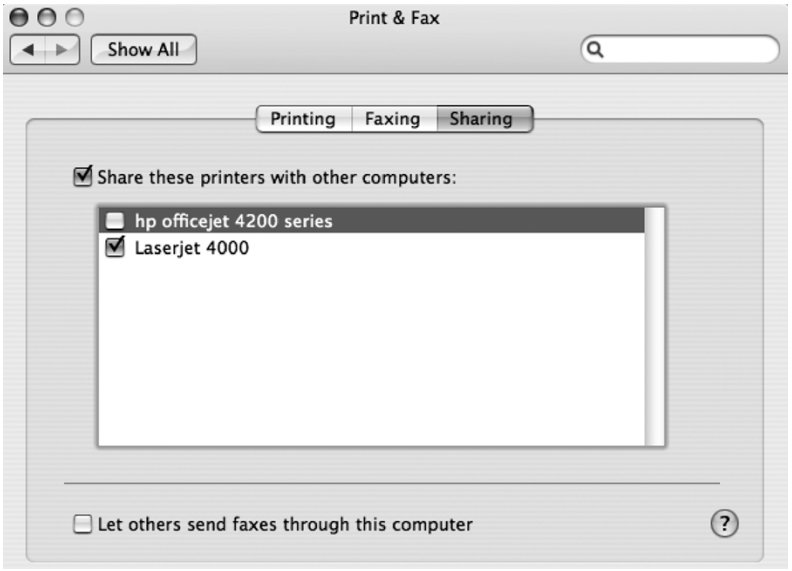

Figure 1-19. *Printer sharing*

You can get more control over printer sharing by using Terminal or the Common Unix Printing System (CUPS) web interface to configure the CUPS. CUPS uses the Internet Printing Protocol (IPP) to provide printing services to users. The CUPS daemon is controllable through a variety of mechanisms such as configuration files and web interfaces, which is convenient but also not entirely secure. If you do not need to allow access to printers installed on your computer, it is best to leave printer sharing disabled.

If, however, you do need to give access to printers on the computer but you want to limit this access, CUPS via the web interface can be helpful. CUPS uses HTTP as its transport protocol and has a built-in web interface to allow configuration of the service. To access the web interface, type the address **http://127.0.0.1:631** into your web browser (see Figure 1-20). The CUPS server has a configuration file that is editable from within the CUPS web interface. Security settings that can be altered by editing this file include the following:

- MaxCopies
- Port
- BrowseAllow
- BrowseAddress
- SystemGroup
- The Location's directive's Allow option

■ **Note** The Location directive has an Allow option that can be used to dictate which addresses are allowed to access shared printing and remote administration.

- AuthType
- AuthClass
- The Limit directive's Require User option

■ **Note** The Limit directive has a Require User option that dictates what access various users have. You should limit users' access on an "as-needed" basis.

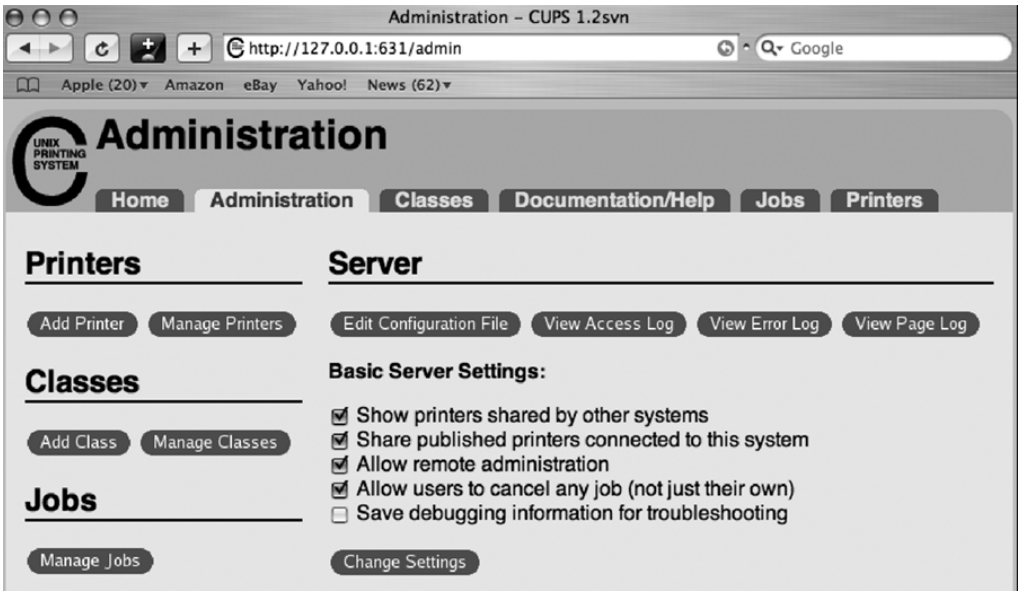

Figure 1-20. *CUPS web interface*

Sharing Services

If you are not sharing any resources on your computer, disable any sharing services that might be running. To do this, open the Sharing preference pane, and review the items on the Services tab that are being used to share resources (see Figure 1-21).

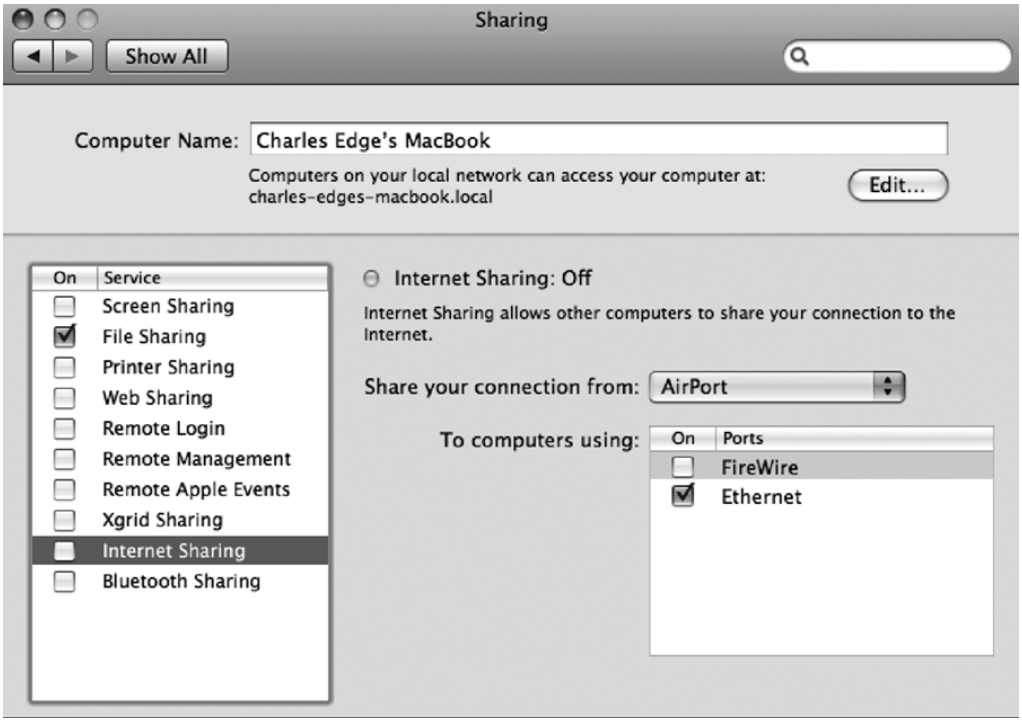

Figure 1-21. *Sharing preferences*

Tip Disable all services that are not needed by the user you are configuring access for. These services are more comprehensively discussed in Chapter 10, Chapter 11, and Chapter 12.

Securely Erasing Disks

When you delete a file from a hard drive, the file is marked for deletion but is often kept by the file system until the system needs to free up space for new files. When you format a hard drive, something similar occurs. To ensure that data isn't accessed by malicious users, always securely erase a disk before disposing of it or repurposing the drive.

To securely erase a disk, open Disk Utility, and click the drive in the left column. Next, click the Erase tab, and then click the Security Options button (see Figure 1-22).

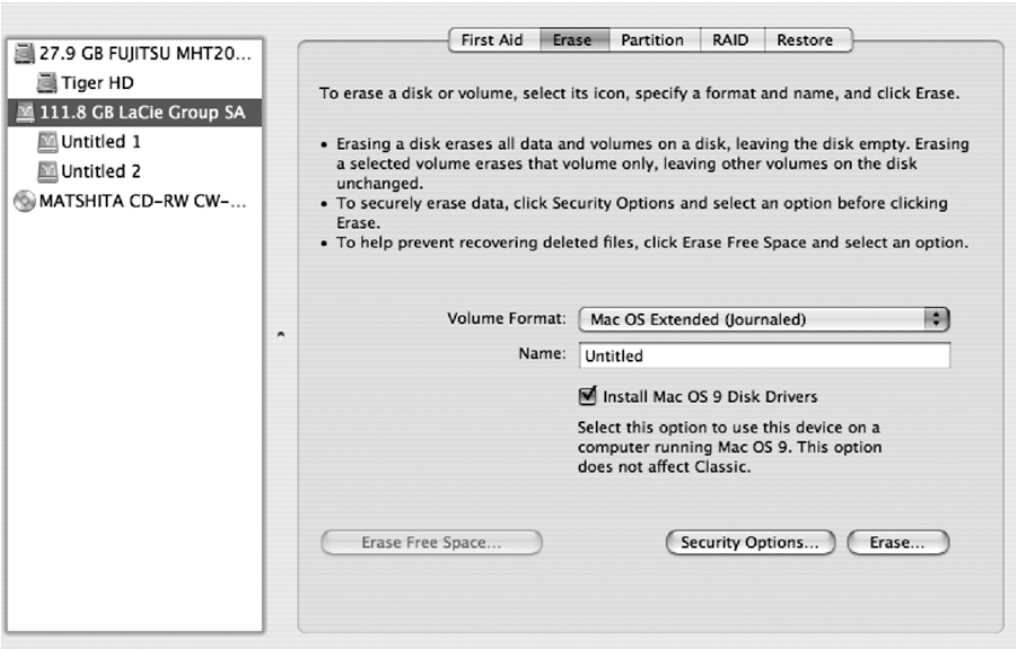

Figure 1-22. *Erase feature of Disk Utility*

This will display a list of secure erase options (see Figure 1-23). The Zero Out Data option will write zeroes over the entire hard drive. This can take minutes to hours depending on the size of the drive. For those needing a more secure erase option, Mac OS X also has a 7- or 35-pass erase available. These options will write data onto every sector of the drive in the number of passes selected. This can take tens of hours for larger drives but will yield a more secure removal of your data, rendering it virtually impossible to extract data from the drive if it were sent to drive recovery.

■ **Note** Make sure you no longer need the data before performing any erase options. Once you have erased it, the cost of retrieving the data will be great, if it is even possible.

Figure 1-23. *Secure Erase window*

Using the Secure Empty Trash Feature

The Secure Empty Trash feature works much the same way as the Secure Erase feature. This is more secure than simply emptying the trash in that it also overwrites the location of the hard drive where the data in the trash was stored with random data. This will cause the data to be much harder to recover if it were to fall into the wrong hands. To securely empty the trash, click Finder ➤ Secure Empty Trash (see Figure 1-24).

Figure 1-24. *Secure Empty Trash menu item*

In Finder, click the Secure Empty Trash screen, and then click the OK button to make the files unrecoverable. It is worth noting that there are a variety of popular applications to help undelete files. As Figure 1-25 states, by clicking the OK button to securely erase your trash, you will not be able to recover the files at a later date, even with these data recovery applications.

Figure 1-25. *Secure Empty Trash confirmation*

Using Encrypted Disk Images

Encrypted disk images offer you a place to keep files in an encrypted form. You can use these if you do not want to keep your entire home folder encrypted as you would with FileVault (likely because of speed or compatibility issues). Encrypted disk images are much like ZIP files that compress a bunch of files into one file, but anyone attempting to access the data within them will need a password to do so.

To create an encrypted disk image, open Disk Utility, and click New Image in the toolbar. The following screen (Figure 1-26) will have a wide variety of options. The Volume Size and Encryption settings are the most important to consider when creating the disk image. The volume size determines the size limit of the disk image. The encryption type can be 128-bit or (for more security) 256-bit; 256-bit images are harder to crack, but they are slower to create and to open when created. They will also take up more disk space than 128-bit. It's important to consider whether 256-bit encryption is worth the performance hit and disk space increase you will experience from using it.

■ **Note** If you are unsure what the size of your disk image should be and are not worried about limiting its size, choose Sparse Disk Image from the Image Format options, and the image will automatically grow as it requires more space (such as when you add files to it).

When you click the Create button, you will be asked for a password. Next you will click the Create button, and OS X will create a file using the encryption algorithm you have selected. Once you have created an encrypted disk image, you will need the password anytime you need to access that image.

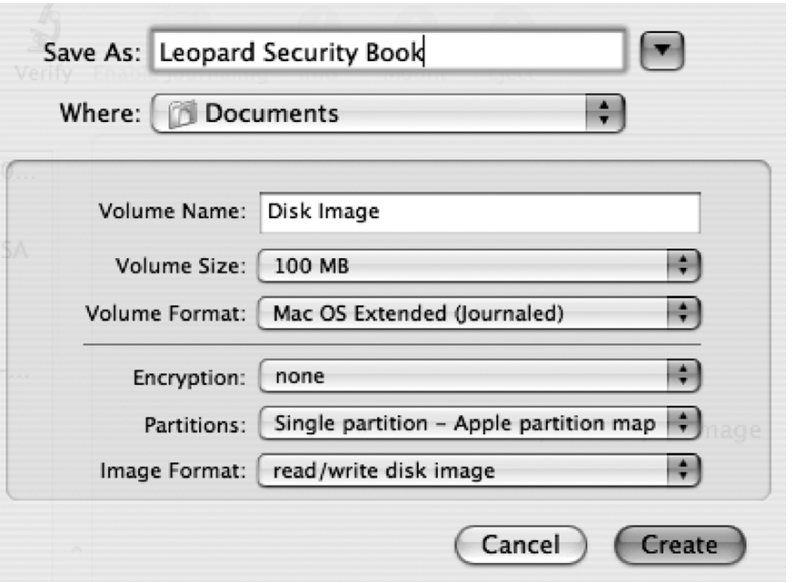

Figure 1-26. *Encrypted Disk Image options*

Securing Your Keychains

Mac OS X uses encrypted keychains to keep track of commonly used passwords and certificates that are accessed regularly. It is meant to make your life easier by automating the manual reentry of this information every time you need to access it. One keychain password can be used to unlock a number of passwords, allowing your computer to keep track of credentials, saving you time, and allowing you to not have to keep track of them yourself. This is also helpful in that it allows a single service to maintain a centralized database of passwords, rather than having each application ask for passwords. This provides a substantially secure way of caching passwords for future use. But it's secure only if used correctly. When setting the keychain password, make sure to use a difficult password to crack that is unique from all the other passwords on the machine.

■ **Note** You can use the Keychain Access Utility to view and manage keychains.

It is possible to have multiple keychains, and each user will begin with their default keychain stored at `/Applications/Utilities/Keychain Access`. When you open the Keychain Access Utility, you will see four panels. The first, labeled Keychains, lists all the keychains on the system known to the Keychain Access Utility. From here you can lock and unlock keychains by clicking them and clicking the lock icon at the top of the screen (see Figure 1-27).

Figure 1-27. *Keychain Access options*

You can create new keychains by clicking Open Keychain Access and clicking the + sign on the next screen. This essentially creates an encrypted disk image file containing other information that needs to be secured, such as cached passwords to web sites. The password assigned to each keychain will open the disk image, thereby unlocking the keychain. Each keychain can and should have a different password.

Best Practices

To wrap this chapter, here is a "cheat sheet" of some of the most important practices you should employ in keeping your Mac secure. Some of these will be covered in later chapters:

- Install antivirus software (see Chapter 4).
- Always install Apple's security updates.
- Open files only from known sources (see Chapter 10).
- Use a standard account for everyday work (see Chapter 3).
- Disable automatic login, and assign a password for every user (see Chapter 3).
- Lock your screen when you step away, and require a password to unlock it.
- Give your keychain its own password, and lock it when it is not in use.
- Use a firewall (see Chapter 8).
- Encrypt important files.
- Protect your wireless network with WPA, and use VPNs when using public wireless (see Chapter 9).
- Protect sensitive e-mail from prying eyes using encryption (see Chapter 5).
- Practice private surfing (see Chapter 5).
- Encrypt your chat sessions (see Chapter 5).