Apple has lost its glorious security period?

With the largest number of security patches and vulnerabilities in wireless device support, Mac OS X operating system seems to no longer extend its championship period. Our experts have studied the threats

With the largest number of security patches and vulnerabilities in wireless device support, Mac OS X operating system seems to no longer extend its championship period. Our experts have studied the real threats in the Apple world and outlined some simple steps to help you protect yourself.

The first highlight was Apple's relatively large May security update, patching more than 40 bugs in Mac OS X and QuickTime operating systems. Then the August patch with more than 26 bugs fixed. Almost at the same time, the research experts profoundly mentioned the vulnerability of wireless device security vulnerability in MacBook computers at this year's Black Hat hacker conference.

What is happening? Is Mac OS X ending your glorious period? Are there a large number of ' *Windows-level* ' security issues that appear in Mac OS X following the normal behavior of operating systems?

Not so. Research from MacBook computers is hacked, security experts claim that defective drives are third-party wireless access devices, not built-in AirPort cards in the MacBook.

If you do not encounter silly security errors, OS X is as safe as before. The phenomenon you are seeing is the natural development of operating system security issues. It is becoming more popular.

Secure Windows and Mac security

Mac OS X is a very secure operating system. But that doesn't mean it's absolutely magical. Some Mac users prefer to spread the myth of 'the perfect security of Mac OS X'. But in fact it is just one of the well-designed operating systems. Mac OS X is highly resistant to threats, but does not mean there is no vulnerability to attack.

It is also not right to say that Windows is the worst operating system. In the beginning with Windows NT 4, Microsoft Office and Internet Explorer, Microsoft took bold steps with tough decisions. If there is no bad reaction from users, they will create *nigh-crippling problems* as you see in today's Windows operating systems. The worst thing about Windows is that the system administrator's *Admistrator* account and too many software packages for this account. The Windows *Administrator* account is the same as the strongest *root* account on Unix. There are no files that the administrator is not allowed to access, no administrator activities are not performed. Even this account is set by default in all Windows operating systems, from NT to XP. So every time you use a computer with some original download, you'll be . king. There is nothing you can not do. You don't even have to receive any warnings.

Adding a very insecure point is the habit of Windows, the operating system does not even require a password for the *Administrator* account. You can perform the login process automatically, without using a password. So malware when entering the system can run as a *root* (*root* account). Very few operating systems can prevent software programs from running with such privileges.

Apple has no such thing. A user with the ' *Admistrator* ' role has no root account privileges, but only in the ' *admin* ' group. That means, when needed, users can authenticate and run the program as a *root* (*root* account), but it is basically not a real *root* . In Mac OS X, the ability to login the system as a *root* is not possible. You must perform some setup steps before you can use this function.

Microsoft also learned some details from Apple in Windows Vista. When the operating system is released next year, users will not be allowed to log in as an *administrative* or *root* by default.

Reason of all patches?

Mac's security warnings and recent patches are not a sign that Apple is confusing operating system security. But

many people are still actively looking for vulnerabilities so Apple can patch them. Ironically, all of this has been confirmed by Synmatec in many reports in 2005. In the ' ***Internet Security Threat Report*** ' article, Symantec claims that Mac OS X is on more and more popular, many people will find their vulnerabilities (strong or weak). And so, of course, the number of vulnerabilities found will increase and that's what you see today.

That is not bad. It may be a bit worrisome, but that is the best way to reduce the vulnerability. If those looking for Mac OS X vulnerabilities are just Apple employees, the operating system will still have many errors missed. These holes themselves are not easily exploited directly. They are just a potential route to exploit and that's why you need to keep the latest version of your system up to date.

The truth is that all malware has so far not paid much attention to OS X and you're still not in the danger of doing a few common protection steps. Real threats in the Mac world are just smug and foolish actions.

Protect yourself

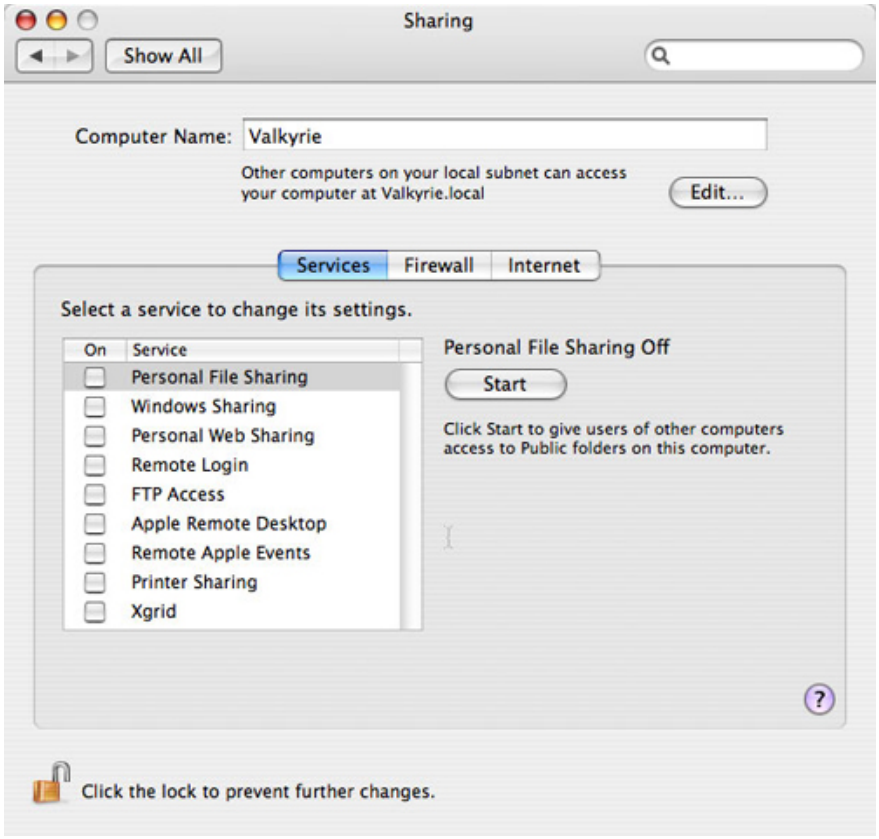
Although Mac OS X is quite secure, you can also take some of the following easy steps to protect yourself:

1. Do not use the Sharing function unless you need to share the file.

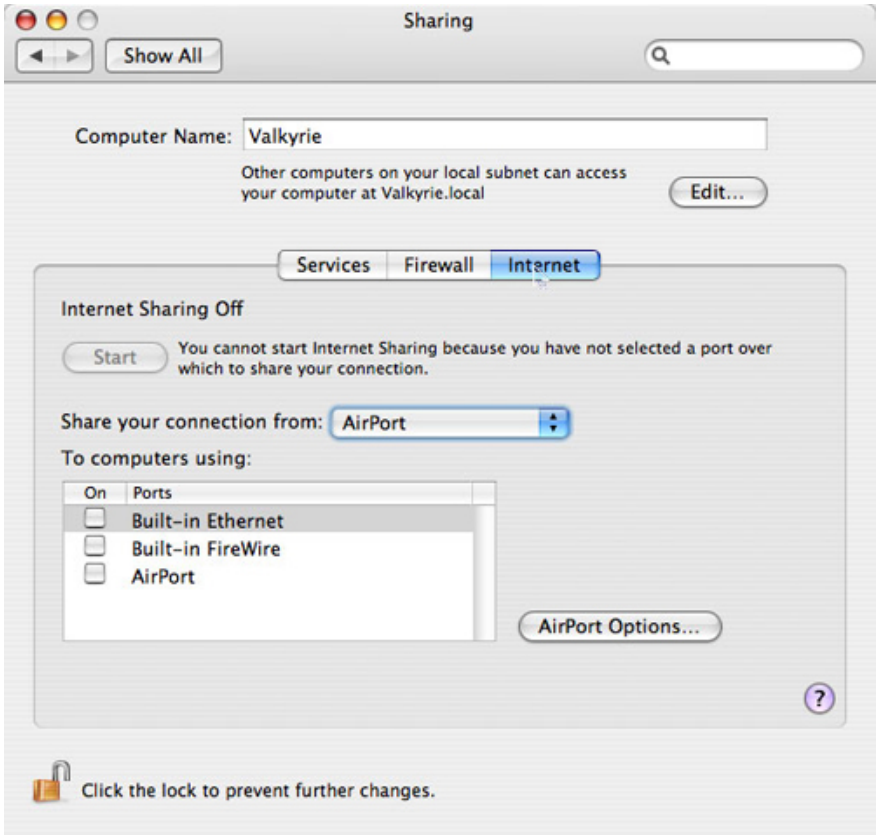
Unless you really need to share files with someone, you need to enable Sharing. This is a very easy step. There is no need to do anything. By default, all shared services in Mac OS X are in 'disabled' mode (not in use). The attacker will be much more difficult if he wants to transfer a file to the machine that never opens the file transfer path.

If you are not sure whether you need to share the file or not, you can consider following the instructions: If you have to ask ' *Should I do it* ', the answer is ' ***No*** '. If you need to do something, be sure of it.

In the two illustrations below, you can see the default security sharing settings. If you enable any sharing service, you are not sure if they still work. These are things you should know when turning off these services. (The Sharing dialog is the first dialog you see in the *Sharing Preference Pane* section in the *System Preferences* section)



Set default file sharing (off) (*Source:* ***InformationWeek***)



Set default internet sharing (off) (*Source:* ***InformationWeek***)

2. Don't download strange software

Don't download strange software, which doesn't mean 'never download anything without the full source code' but you should be sure of its source. As before, a group of people who had a catastrophe said they were downloading the free Microsoft Office 2004 demo internet. While it was actually a malicious script, it erased their root directory. Of course there is only one place for these scripts to exist that download websites must ask questions like Limewire.

In general, download software from trusted websites like VersionTracker. It's a great website, not only for Mac OS X but also for Windows and Palm. They are also updated daily. Unlike most P2P networks like LimeWire mentioned above, VersionTracker does not allow posting anonymous software on the website. And at least one basic testing program of software will be posted on the website.

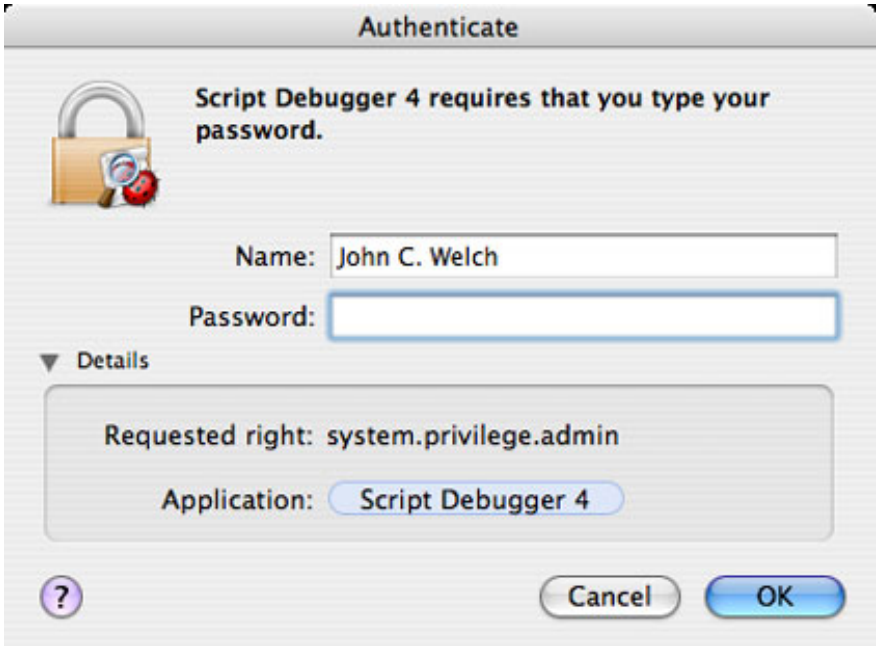
No one can guarantee perfect safety. But VersionTracker has so far chosen a reasonable security method. Download it now, but the process of running the new program should be the most careful. Because every time you run the code, you can't control what the code is doing. If you are an administrator, the source code is for you. If you verify as a root in a security dialog box, the source code runs as a root. Nothing in this world can prevent a Trojan horse with original privileges.

3. Think before entering the password

Many applications require you to enter an administrator password, especially during the installation process. But you should not do that right away. There is always a reevaluation question. If nothing happens, check to see if the required dialog box is valid. Here are two images that require authentication authentication I created with Applescript to prove:

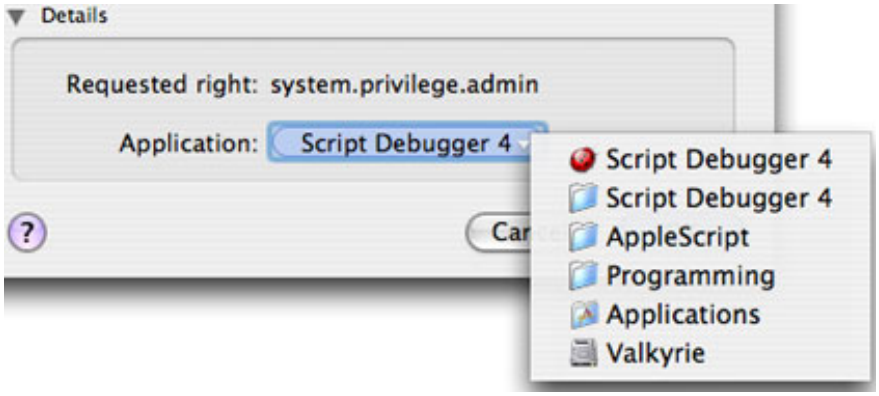
Check to see if the required dialog box is authenticated before accepting it (*Source:* ***InformationWeek***)

There are several ways to determine if this is a dialog box that requires authentication. The first is the lock icon with the application icon required above. Then the message line, telling you the application (in this case, Script Debugger) is asking for your password. Next is the full username already filled in the 'Name' box. If we expand the 'Details' triangle we will see more information that can help you.



Make sure the application name matches . (*Source:* ***InformationWeek***)

Now we will look at the specific requirements of an application (system.privilege.admin) when allocating access privileges as a root. If the name of the application does not match the icon name at the top of the dialog box, think twice before performing the confirmation. However, you should first check the privilege location that requires the application. If you click on the blue border of the application name, you can get the link to the application list, as shown below:



. and see if the file path is appropriate (*Source:* ***InformationWeek***)

The path shown in Debugger Script 4 is exactly in the directory: / Applications / Programming / AppleScript / Script Debugger 4 / (note in Unix the '/' prompt indicates the root level of the boot drive, and the directories shown with a slash '/'). If the path shown in the dialog box and the path of the application should be different, you should not enter the password.

Checking the dialog box is not a perfect method, if not quite trivial, but it is better to have something to check than to blindly trust.

4. Update patches.

While you may not want to insert patches for heavy machines, I don't wait more than a week to update it. Security patches are the simplest way to protect yourself. I always update the operating system version although you may have to pay for the new version because the fact that the current version always attracts more attention when an error occurs and a fix. Security is the best reason to update new versions. Some security vulnerabilities may require changes that only the new operating system version can resolve.

If you follow these four tips and apply a common sense in daily Mac manuals, the chances of solving problems will be much faster.

There will be no big security nightmare from Mac OS X anymore. All just want to say is that more people will use Mac OS X and Apple will take more seriously from the point of view of security. And finally everything is fine!