Global Information Assurance Certification Paper

OS X Security (10.3)

Security “for the rest of us”

By Michael Puddington
8 October 2004
GSEC Practical Assignment 1.4c, Option a

Abstract

When the Titanic was launched, its owners considered it to be “practically unsinkable”. There are echoes of this in the Macintosh community with the widespread belief that the Mac OS X is similarly “unsinkable” with regard to viruses and other security issues. This document will examine different aspects of security on the Macintosh platform and will outline steps that users and administrators can take to help ensure that their systems remain “shipshape”.

This document will cover the following topics:

- Physical security
- Access to the machine
- User accounts
- Password management
- Patch management
- File security
- Anti-virus
- Email
- Networking (including personal firewalls, intrusion detection, and wireless)

Physical security

The Macintosh is considered by many people to be a desirable computer to own. Over the last few years, the G5, the PowerBook, and, especially, the iMac have redefined their particular categories in large part through their cutting-edge design. Apple has won many awards for its pioneering work in this area. One unfortunate downside of the "desirability" of Macintosh computers is that it also makes them attractive to steal. There are a few simple steps that people can take to minimise the risk of their computer being stolen.

The first step is to reduce the visibility (or, to a potential thief, the 'availability') of the computer. For a G4 or G5 tower computer, this can be done by placing the CPU under, rather than on top of, one's desk. For a PowerBook or iBook in an office or home environment, reducing visibility means putting the computer in a drawer (preferably one that can be – and is – locked) when the computer is not being used. When travelling, it's best to be discreet about using a PowerBook or iBook. Those who need to use a computer in public (for example, at a café) should position themselves away from pedestrian traffic in order to reduce the risk of the computer being snatched by a passer-by. When the computer is not in use, it should be kept in a bag or case (it's more effective if the bag doesn't look like a computer bag), and keep the bag close at hand.

The second step is to make the computer more difficult to remove. For a G4 or G5, the CPU can be placed in a secure enclosure that still allows air to circulate, but that restricts physical access by using a lockable door (for example, http://www.computersecurity.com/lockdown/enclosures.htm). Although iMacs and eMacs are more difficult to "hide", they can be secured to a desk with a lockable plate (for example, http://www.computersecurity.com/lockdown/macplate.htm). In the office or on the road, users of PowerBooks and iBooks should use a security cable – a simple, low-cost accessory that can be used to secure a laptop (or a desktop computer) to a fixed object. Although the cables can be cut by someone with the appropriate tools (for example, a well-equipped thief), they can act as a deterrent, particularly to the "opportunist" thief who might take a computer if it looked like it would be easy to steal but who otherwise would not be interested.

The final, and perhaps most drastic, step is to reduce the attractiveness of the computer itself. "Branding" the computer in a very visible place with a non-removable etching or burnt-in stamp with the owner's contact information can be an effective deterrent. The key is to ensure that potential thieves see the stamp *before* they take the computer. It acts as a deterrent because thieves will find it more difficult to resell the computer – scrupulous potential buyers would typically use the contact information and follow up to see if the computer was stolen. The unfortunate downside is that the computer may be more difficult to sell for the rightful owner, too!

Access to the machine

System Preferences

There are a few steps that one can take to protect the integrity and confidentiality of the data on a Mac from someone who has physical access to the machine.

These steps will hinder, if not prevent, an unauthorised person gaining easy access to an account on an unattended computer.

The “Security” System Preference has an option to “require password to wake this computer from sleep or screen saver”. It is prudent to enable this and to configure Mac OS X’s built-in screen-saver to start after a relatively short time of inactivity. NB: the credentials for an administrator account *will* succeed in gaining access to the currently logged-in account (eg User X); users who have a non-administrator account on the computer would be able to login to their own account using their credentials, but they would not be able to access the User X account.

Also in the “Security” System Preference, “automatic login” should be disabled for all accounts on the computer – clearly, a computer is not very secure if someone can gain access to it simply by restarting it!

In the “Accounts” System Preference, “Login Options” can be configured to display the login window as either a list of users or fields that require someone to enter the name and password. With the ‘list of users’ setting, people trying to gain access can see the valid usernames; they just need to guess the password. The latter option is more secure because people trying to gain access would need to guess both a valid username and password.

Open Firmware

It is possible to tighten the security on a Mac further by enabling Open Firmware security. “With the release of the Firmware 4.1.7 update, Apple made it possible for certain Macintosh models to use password protection before the computer starts up. This protection method is similar to the BIOS password protection used on PC computers.”[i] (Apple does not recommend using Open Firmware with any version of the Mac OS earlier than 10.1.)

When Open Firmware security enabled, the computer will require the entry of the Open Firmware password before the computer will boot from a CD, from a NetBoot server, or from an alternative boot device; a password will also be required to boot into single-user mode, verbose mode, Open Firmware mode or target-disk mode (target-disk mode makes a Mac available as an external hard drive when connected to a different computer).

The Open Firmware password is stored in NVRAM. Although the password protection can be removed by resetting PRAM, the PRAM cannot be reset without first changing the amount of RAM in the Macintosh (or by entering the Open Firmware password). Therefore, someone would need the appropriate knowledge or extended physical access to the Macintosh to circumvent this security; even in these circumstances, however, it will help to slow down the attacker. Note that the Open Firmware password can also be reset by an administrator or through booting into OS 9.

Remote control software

Users can gain access to a Macintosh without requiring physical access if they are able to connect to the computer remotely via software such as Timbuktu, VNC, or Apple Remote Desktop (see also Patch Management). These software

programs can be invaluable tools for IT staff; however, they should be deployed with great care so as not to compromise security.

In general, it is advisable to require the permission of the "host" to allow the "guest" to connect (obvious exceptions would include systems where there is typically no one there to "answer"). This act of courtesy alerts the host and makes it explicit that someone is connected, reducing the risk of them displaying confidential information.

Visitor privileges should be defined for named accounts (as with the OS, it is good practice to avoid the use of generic or "functional" accounts such as "helpdesk" or "finance"). The principle of "least privilege" should be heeded: if IT staff use Timbuktu to assist users, then it may be appropriate for them to be able to observe and control a machine but not to be able to delete or transfer files from the host machine.

User accounts

The principle of "least privilege" applies to user accounts as well: it is recommended that normal user accounts be defined to exclude "Administrator" rights. It's perhaps so obvious that it might be overlooked: all accounts should have secure passwords (or passphrases): at least 10–15 characters (the longer, the better), include non-letter characters (ie punctuation and numbers) and minimise use of dictionary words.

Admin

Having a single occasional-use administrator account can be helpful (it's also necessary – there has to be at least one administrator account on the machine); user accounts do occasionally become corrupted, and it makes troubleshooting a corrupted account much easier if one can login to a different account on the machine. Because multiple administrator accounts have equal privileges, there is no significant benefit in having more than one, or in giving end-users administrator rights. Instead, create user accounts for each person who needs to administer the machine, and have them use the **sudo** command to temporarily assume the rights of the administrator; a benefit of this is that it provides an audit trail – the use of sudo is recorded in the system log.

Root

Because OS X is based on UNIX, it is possible to enable the omnipotent "Root" account. From a security point of view, enabling this account is generally considered "a bad thing" to do, as it significantly increases the possibility of a hacker exploiting Root's access to all parts of the system. By default, Apple ships OS X with root disabled, so anyone with administrator rights can enable it. Arguably, this is slightly more secure than assigning a default password, but it's not ideal. In any case, "the first thing to do on a new system is to enable and set the password for Root by using NetInfo Manager. Once you set up Root the first time, then you can disable Root access."[ii] This improves security because even if a would-be attacker gained access as an administrator, the attacker would still need to know the Root password to gain access as Root.

Password management

Mac OS X includes Keychain, Apple's password-management software. Keychain can store username and password information about multiple resources, so a user can "unlock" multiple resources by validating the Keychain. It is reassuring to know that the information is stored as encrypted data; it is only decrypted when needed. There is a downside of Keychain: depending on how Keychain is configured, users may be more prone to forget their passwords because they are not being prompted for them (in effect, Keychain does the work of remembering on the user's behalf). When people do need their passwords – for example, if they are using a PC or another computer where they don't have access to their Keychain – they may find them more difficult to remember. On balance, however, Keychain improves security. People often find it difficult to remember multiple user names and passwords for different systems; as a result, they often use the same password for many resources (or worse, write down their passwords on a Post-It note on their monitor or under the keyboard). By managing multiple user names and passwords, Keychain makes it easier for people to work with different passwords for different resources.

One important note: if someone has access to your unlocked Keychain, or if they discover your Keychain password, it's as though they have a master key, so it's important to minimise the risk of unauthorised access. Configure the Keychain settings (use the Keychain Access utility) to lock after a relatively short period of inactivity and to lock when sleeping. With this tool, it's also possible to configure each resource password to determine whether Keychain is allowed to provide the information or whether it requires the user to confirm (for example, by having to enter the Keychain password).

Patch management

The Macintosh OS, like all systems, has security vulnerabilities and other flaws. For the year 2004 to date, the United States Computer Emergency Readiness Team web site lists vulnerabilities for twelve different issues on Mac OS X.[iii] Although they generally receive less publicity than similar issues on Windows machines, these vulnerabilities do represent a risk to security, and it is important that they are addressed as quickly as possible. (The release of a patch to address a security vulnerability often acts as a "flag" alerting hackers to the presence of the vulnerability. It is common for hackers to write code that will exploit a newly-identified vulnerability, so the sooner the patch is applied, the less chance the hackers have of exploiting the vulnerability.) Vulnerability notes often list patches, tools, and workarounds that are available to address the vulnerabilities. The prudent user or administrator will monitor security sites on a regular basis and/or subscribe to one or more authoritative security mailing lists.

Over the last year, Apple applications such as Safari, iChat, and the Apple Help Viewer have been shown to have vulnerabilities. Apple is not alone, however: the Secunia web site lists vulnerabilities in Macintosh software from Mozilla/Netscape, Microsoft, FileMaker, and Macromedia, among others.[iv]

The message is: be vigilant – check regularly for vulnerabilities concerning applications as well as those concerning the OS, and when vulnerabilities are identified, address them quickly.

To tackle the challenge of patching Mac OS computers, users and administrators can choose from a handful of tools, from higher-end, multi-platform solutions to lower-end, Mac-only solutions.

Software update

Apple had the foresight to include a "Software Update" facility in OS X. This mechanism can be configured via "System Preferences" to check for software updates on a regular basis (daily, weekly, monthly) or manually. Although the updates and patches it retrieves are Apple-only, it is an effective mechanism for ensuring the core OS and Apple-developed applications are kept up-to-date. To ensure that the "window of opportunity" for an attack on a vulnerability is minimised, it is good practice to configure the system to check for updates at least weekly, preferably daily. The "Software Update" facility also provides the ability to download important updates in the background, reducing user intervention and speeding up the installation process.

To install a software update from Apple, it's a common requirement that an administrator's username and password must be entered. This helps to ensure that end-users are not able to install software and/or updates that have not been tested or approved; the downside is that it requires an administrator to intervene on each machine. In sites with more than a few Macintosh computers, this may prove impractical, and it may be preferable to use a tool such as Apple Remote Desktop (see below). Other drawbacks with Software Update include the fact that each machine downloads its updates from the Internet – it's not possible to point Software Update to a local server. Apple has so far shown no willingness to provide this functionality, or to open the tool up to be able to receive software updates from other software companies.

Apple Remote Desktop

Apple Remote Desktop (aka ARD) is a relatively low-cost tool (approx. $500 for one administrator and unlimited clients) that can help to simplify the administration of multiple Mac OS computers. In the area of patch management, it makes it possible to push out approved updates to multiple computers without the need to visit each machine. By centralising the downloading, testing, and administration of software updates, ARD can give administrators greater control than with Software Update. For example, administrators can download and evaluate updates (from any source, not only Apple) in a test environment. Once they approve the updates, they can push them to the remote computers ARD, avoiding the need for each client to download the updates from the Internet. ARD can also be used to gather information about what version of software is installed on different computers, making it easier to identify which ones need to be updated.

Other alternatives

Like Apple Remote Desktop, both FileWave and radmind have the ability to deploy software updates to multiple machines. FileWave is a commercial product that has evolved over many years; it received a major overhaul for OS X.

Radmind is newer to the Macintosh world. An open-source tool from the University of Michigan's Research Systems Unix Group, radmind has been compiled to work with OS X; there is a GUI to simplify dealing with the command-line tools. Although both tools are arguably more difficult to use than ARD, they offer some added security benefits in that they can compare client systems with a benchmark and restore them to the standard configuration. For example, administrators "can use radmind to combat any application or system corruption and even deliberate misconfiguration by simply running the radmind update session. When used with checksums, radmind also verifies the integrity of files and any damaged ones are replaced."[v]

Both tools can be used to administer non-Mac platforms: FileWave can manage Windows clients, and radmind can manage some UNIX-based systems. For business customers, FileWave is not a cheap option; for education customers, reduced pricing is available. Radmind is available with a BSD-style license (in layman's terms, it's free). Both products require a significant investment in learning and pre-deployment planning.

The major players in the enterprise patch-management market have been a little slow to embrace the Macintosh. Novadigm, Marimba, and PatchLink all purport to offer Mac OS support; PatchLink's "PatchLink Update 6" product appears to be the most fully developed offer.

File security

FileVault

With Mac OS 10.3, Apple introduced a security feature called FileVault. If a user has FileVault activated, that person's Home folder is encrypted using the Advanced Encryption Standard (with 128-bit keys) and saved as a disk image file – anything contained in the Home folder is not accessible unless that user is logged in. While the user is logged in, FileVault mounts the disk image and then decrypts and encrypts files as they are accessed; this is transparent to the user. Administrators can – and should – set a "master password" for each computer where FileVault is used; this enables them to access the data *in extremis*, for example if users forget their password.

Whereas enabling Open Firmware Security and requiring a password when waking from sleep are less effective if someone has extended physical possession of the computer, FileVault security is robust enough to provide protection even if the disk it is protecting is physically removed from the machine. "Even though it doesn't prevent hackers from accessing the hard drive and reaching the Home folder, it does make the contents of Home a pile of nonsense, unless they can crack the encryption or guess your password."[vi] Apple's humble Disk Utility also enables users to create encrypted disk images. These can be "mounted" and used in a similar way to real disks. This can be helpful if people want to encrypt some, but not all, of their data. The disk images can also be transferred from machine to machine.

The PGP Corporation's PGP Corporate Disk and PGP Personal Disk products provides much of this same functionality, although it is not integrated into the

operating system. They can, however, be integrated with PGP's encrypted mail solutions (see below). A freeware license is available for non-commercial use.

Trash

We have all heard tales of how second-hand computers have been found to contain confidential information – a few years ago, information about Paul McCartney's personal bank dealings was found on a PC sold by a computer disposal company.[vii] An easy way to ensure that you don't end up as a multi-millionaire whose banking details have been compromised (doesn't sound that bad, actually) is to use the "Secure Empty Trash" command. Instead of simply erasing the information about the file, this wipes the data itself in a very secure way. How secure? Well, secure enough to meet the U.S. Department of Defense standard for the sanitization of magnetic media.[viii]

Anti-virus

Although the Mac OS X is not a common target for virus, worm, or Trojan horse attacks, these kinds of security threats do represent a tangible risk, and any sound security strategy for Macintosh computers should ensure that anti-virus software is installed on every machine.

Enterprise solutions

Symantec has announced plans to release, before the end of 2004, a Web-based console to enable central administration of Macintosh clients licensed for Norton AntiVirus for Macintosh 9.0. [ix] Though perhaps less well known, CA's eTrust Antivirus product provides the ability to manage clients on a variety of different platforms (including Mac OS X) from a central console. Sophos also offer the means to manage heterogeneous client environments with their Sophos Anti-Virus product range. Administrators of medium- to large-scale sites should find that using one of these three products would simplify the task of managing their anti-virus operations.

Other alternatives

Virex, from McAfee, does not offer the central administration capabilities of the products above, but it has been a market leader on the Macintosh platform for several years. Other options include Intego's VirusBarrier, or CLAM, an open-source anti-virus tool that has been ported to the Macintosh.

Email

Email has become so commonplace that it's easy to forget that it is transmitted relatively insecurely. There are two relatively straightforward ways to address this: signatures and encryption[x]. The former vouches for the authenticity of the sender and the integrity of the message (ie it hasn't been tampered with); the latter prevents the message from being read en route.

Certificates can be obtained from a variety of certificate authorities: VeriSign and GeoTrust charge a small fee; Thawte and CAcert provide them for free. James Huff has written a useful article on MacMerc.com (http://www.macmerc.com/articles/Power_User_Monday_Tip_of_the_Week/226) describing how get set up some common email applications with certificates. Apple's Mail application, Eudora, Microsoft Entourage, and Lotus Notes all

support the use of certificates. The PGP Corporation's "Desktop" range of software provides some additional functionality including the ability to encrypt attachments and instant messages (you'll remember from above that this can be integrated with their disk security products).

Networking

Personal firewall

It's a big, bad world out there, and to ensure it stays "out there", it is good security practice to deploy personal firewall software on any Macs that are not protected by a corporate firewall. Obvious choices to run personal firewall software are home Macs or corporate PowerBooks that are used outside the office. Vigilant administrators could take the "defence in depth" philosophy further and protect all of the Macs they manage, even if they are behind a corporate firewall, to protect them from rogue intra- or inter-office traffic. Like a corporate firewall, a personal firewall's job is to let "approved" network traffic pass and to block unapproved traffic – this could be between the Internet and the Mac itself or, if the Mac is acting as a router, between different network segments (eg from a cabled segment to AirPort).

Mac OS X includes a packet-filtering firewall based on ipfw; it can be configured via the "Sharing" System Preference pane. When enabled, the firewall takes an "all closed" approach: the administrator must specify which ports should be open to incoming traffic; anything else is closed by default. (While looking in "Sharing", make sure that all but the desired "Services" are turned off, and check "Internet" to make sure that the computer's Internet connection is not being shared unwittingly.) The firewall is clever enough to allow the services you've requested, eg if the "Remote Login" service is enabled, the firewall will open port 22 to inbound traffic.

Those who find the "Sharing" controls too limiting may want to try SunShield, a free System Preference pane that provides much greater flexibility than the Apple tool. SunShield offers network address translation (NAT), the ability to create customised rules, and advanced logging.

There are several personal firewalls available for Mac OS, including commercial offerings from Symantec, the PGP Corporation, and Intego; some of these also offer intrusion-detection capabilities (see below).

Intrusion Detection

Snort, an open source tool, is the *de facto* standard network intrusion detection system. The good news is that it runs on OS X. What does it do? It looks out for suspicious activity on the network and produces logs that can help administrators (this is not a tool for the average user) to identify attempts (successful or not) to hack into a network or a system. The administrator can then decide what action to take. HenWen is a fantastic companion tool that makes it easier to set up and configure Snort by providing a GUI front-end; it's only $25 for commercial use, otherwise it's free.

Intego's NetBarrier and Symantec's Norton Personal Firewall both provide some basic host-based intrusion-detection (as opposed to network intrusion detection)

features. For a more comprehensive host-based intrusion detection solution, consider a tool such as Tripwire. Although there is no GUI front-end for the open source version[xi], Tripwire will run on Mac OS X, and it provides comprehensive detection of changes to the system. It will compare a system to a reference image and highlight every file that has changed – this can be extremely helpful in verifying the integrity of data (for example, confirming whether an attack has taken place, and if one has, what files were affected). Tripwire is available for OS X in an open source version (http://www.macguru.net/~frodo/Tripwire-osx.html). There is a more fully featured commercial version (http://www.tripwire.com), but it is not supported for OS X. Remember that radmind (see "Patch management" above) can also provide some tripwire-related functionality in that it can restore systems to a standard configuration.

FTP/SSH

Apple has thoughtfully included secure shell (SSH) software in OS X to enable secure terminal and FTP communication with remote computers. For those who prefer to avoid using the command-line, consider Fugu, another open-source tool from Research Systems Unix Group, the people who created radmind. Fugu provides a GUI for the SFTP client and also provides SCP (secure copy) and SSH functionality. For more information about Fugu, go to http://rsug.itd.umich.edu/software/fugu/

Wireless/AirPort

Apple helped to popularize Wi-Fi technology through its AirPort product range. Many people would like to take advantage of the flexibility and convenience of Wi-Fi; a good set-up is one that is built with security in mind. Apple's original AirPort cards and AirPort base stations only support the older, less secure WEP (Wired Equivalent Privacy). Their AirPort Extreme and AirPort Express range support the newer, more secure WPA (Wi-Fi Protected Access). Many third-party hardware solutions also support WPA.

A helpful article on Apple's support web site explains how to password-protect a wireless network. http://docs.info.apple.com/article.html?artnum=150715
A more detailed explanation can be found in Wei-Meng Lee's article "Securing AirPort Extreme Networks with WPA" at
http://www.oreillynet.com/pub/a/wireless/2003/12/18/wap.html

If there is a firewall on the network and it supports having a de-militarized zone (DMZ), consider connecting the wireless portion to the DMZ. That way, if someone gains access, they are not on the "inside" of the network. In corporate installations, it may be preferable to deploy a stand-alone DSL connection and connect the wireless network to that; users who need to access the corporate network could do so via a VPN client.

Conclusion

Through a combination of sources – Apple, the open source community, and commercial developers – vigilant users and administrators can minimise security risks to their Macintosh computers. Apple has done a good job of including a reasonable level of security functionality in Mac OS X; other sources have filled in many of the gaps. Perhaps top of the "wish list" for OS X security would be that

Apple would enable Software Update to be developed further, both to enable it to be integrated into a managed solution and to enable it to be used to download software from other sources, not only from Apple. Although Mac OS X may not be “unsinkable”, it can be made quite secure without requiring a Titanic effort.

References

[i] "Open Firmware Security – Introduction". http://www.macosxlabs.org/documentation/firmware_security/intro.html (30 Sept. 2004)

[ii] White, Kevin. "Mission Lockdown - Get Smart With Security Tactics for Mac OS X" http://www.osxfaq.com/Tutorials/lockdown/index.ws (1 October 2004).

[iii] United States Computer Emergency Response Team. "Vulnerability Notes database" http://www.kb.cert.org/vuls/ (1 October 2004).

[iv] "Secunia Advisories" http://secunia.com/advisories/ (1 October 2004).

[v] Gal, Ofir. "radmind Manual for Mac OS X." v.0.40. 5 May 2003. http://www.gal.co.uk/software/radmind/radmind-manual.pdf (1 October 2004).

[vi] De Kermadec, François Joseph. "An Unencrypted Look at FileVault". http://www.macdevcenter.com/pub/a/mac/2003/12/19/filevault.html 19 December 2003. (1 October 2004).

[vii] Cullen, Drew. "Paul McCartney account details leaked on second user PC". http://www.theregister.co.uk/2000/02/09/paul_mccartney_account_details_leaked/ 9 February 2000. (4 October 2004).

[viii] "Security in Mac OS X". http://images.apple.com/macosx/pdf/Security_in_Mac_OS_X.pdf March 2004. (4 October 2004).

[ix] "Symantec Announces Plans for New Antivirus Administration Console for Macintosh". http://www.symantec.com/press/2004/n040916.html 16 September 2004 (2 October 2004).

[x] Huff, James. "Secure Your Email". http://www.macmerc.com/articles/Power_User_Monday_Tip_of_the_Week/226 (4 October 2004).

[xi] Jason. "TripwireTM on Mac OS X". http://www.macguru.net/~frodo/Tripwire-osx.html 14 April 2004 (4 October 2004).

Computer Security Products. http://www.computersecurity.com/lockdown/ (29 September 2004).

Apple Computer. "Password-protecting your wireless network". http://docs.info.apple.com/article.html?artnum=150715 (4 October 2004).

Lee, Wei-Meng. "Securing AirPort Extreme Networks with WPA". http://www.oreillynet.com/pub/a/wireless/2003/12/18/wap.html 18 December 2003. (4 October 2004).