Global Information Assurance Certification Paper

Securing FreeBSD under Macintosh OSX

Bertram McGrath
September, 30, 2001

As the twenty year old Mac OS is slowly phased out in favour of the new, FreeBSD Unix-based OSX, the security picture for networked Macintosh hosts and servers changes dramatically. This instructional paper introduces a broad range of applicable security measures that can be taken to provide a basic level of resistance to intruders, malicious code and damage or compromise to ones PC and/or its electronic contents when using Macintosh OSX.

The original, single-user Mac operating system was extremely secure out of the box. Essentially this is true of all incarnations of the OS since its original inception up to and, for the most part, including OS 9.x.

Why?

Because the original OS was designed to be used by one user only. Also, there was no method of remotely logging into a Mac.

The Mac was designed first and foremost to be user-friendly and very intuitive, allowing for a short learning curve for most operators. It was a daunting, if not impossible task to burrow down into the system guts and find anything like a Unix command line. You had to be a Macintosh programmer to accomplish that feat.

Also, the OS source code was proprietary and not available publically.

With most of the "power controls" under a locked hood, it was difficult for a user to open potential security vulnerabilities. Additionally, the user interface provided "Warning" dialog boxes/messages before permitting critical user-made changes to be made to the system.

As was pointed out by the World Wide Web consortium itself in 1999 regarding web servers, "The safest Web site is a bare-bones Macintosh running a bare-bones Web server."

Now with the advent of OSX, that scenario has changed. Currently, users of OSX are running a dual-boot system which includes Mac OS 9.x, which allows an operator to use their legacy software titles (that have yet to be "Carbon-ised" to run natively on OSX) from within the OSX/Unix environment. In spite of the inherent security of the OS 9 system, all the vulnerabilities of the Unix platform are now open to compromise, and therefore, so is the box itself. In addition, services that have been secured in one of these envirnoments may not necessarily be secured in the other. The passing of this hybrid system, while locking in Mac users to the risks and benefits of Unix, will nonetheless be a welcome one.

So where to begin?

Physical Security

First, considerations of physical security need to be addressed.

Is the PC in a secured physical facility? Locked doors and windows? Physical access controls, alarms, lock-down cables, etc.? These are fundamental considerations for any PC, and should be addressed.

OSX has a log-in security feature for mutiple users as does Unix, which requires a password, though a typically convenient Mac feature, "auto-login", must be turned off. It is on by default. With this feature on, when the PC is booted, your user name and hidden password are already filled in and a carriage return logs you on to the desktop.

It should also be noted that someone with an OSX install disk could reset passwords, or perform a fresh install of the system. This situation assures that a legitimate user will never be denied access to his/her machine, but as a potential vulnerability, it clearly re-emphasizes the importance of physical security for not only the PC itself, but all software also.

Virus Protection

The Macintosh platform has been relatively virus-free for the most part. The AutoStart Worm, which exploited a QuickTime vulnerability, and the AppleScript-based Simpson worm have caused some damage to harddrives and systems as well as creating excess e-mail traffic, and were Mac-only virii. Although the Mac is also susceptible to application-specific malicious code, particularly those exploiting mail and scripting vulnerabilities such as those found in many Microsoft products like Outlook and Outlook Express, Internet Explorer and Microsft Word, the majority of virii, worms and Trojan horses are directed at the Microsoft Windows OS. Unix/Linux variants would be next in line as viable targets.

The install base of Macintoshes is substantially smaller than either of the aforementioned, but with OSX and its Unix underpinnings that base is likley to expand to some degeree. In any case, OSX now puts the Mac in a much more vulnerable position than it has previously enjoyed. Virii and other malicious code now pose potential threats in three ways; attacks aimed at vulnerabilities in Mac's pre-OSX OSs (or "Classic"), those that are Unix based, and any that may be developed specifically for OSX. Particular attention should be paid at this time to Unix-based and application-specific threats and vulnerabilities. Also, bear in mind that AV protection for the Classic environment does not necessarrily provide the same protection for the OSX environment, and vice versa. A myriad of virus protection software is available and needs to be assessed on a case by case basis.

Password Management

As in any computing environment, password management is a key first line of defense in a layered security system plan. With OSX, passwords may be longer than the previous 8 character limit, but most applications and services in both the OSX and the OS 9.x "Classic" environments may only recognize the first eight characters. That will likely change with future versions of some apps. However, by encouraging your users to choose greater than eight-character passwords, they will at least be inadvertantly creating stronger eight-character words.

OSX's built-in screen saver can also be password protected and should be.

The Keychain is a feature in OSX that provides easy access to the multiple passwords users may need throughout the day. Passwords are stored within it and can only be accessed with a "Master" password. While I personally do not recommend putting all my eggs in one basket, it should be noted that by default, the Keychain master password is the same as your log-in password. If using the Keychain feature, change the password immediately. If anyone compromises your stored passwords, they have access to any servers, websites, etc. that you have legitimate access to. If using the Keychain, re-lock it when leaving the computer unattended.

Internet Services (inetd)

Apple has striven to make OSX as secure OOB as possible and practical. Regarding internet services (inetd), they are turned off by default on install. As a general rule, don't turn anything on that you don't absolutely need.

Depending on your preferences, all services can be turned on via the NetInfo GUI without ever touching a text editor or the inetd.conf file. (For those more comfortable editing text files by hand, most configurations can be set up that way.) Caution should be exercised using NetInfo however. While not as complex as the CLI, it is possible to create configurations that may expose the host to undesirable vulnerabilities.

Seriously consider whether or not you need to allow file sharing, remote log-ins or ftp sessions. Do you need to run a web server?

Remote Log-ins can open your machine to users via the telnet daemon. If this is necessary, install SSH, Secure Shell, if using OSX 10.0. SSH became standard on 10.0.1 and subsequent upgrade patches, so if

you're running a revision above that, you have it. SSH encrypts the contents of a telnet session, including session contents, user names and passwords and prevents them from crossing your network in clear text form.

Even so, a potential vulnerability exists by allowing remote access to the full command line interface. If you don't really need it, turn it off. If it is necessary to provide this service, be certain that any authorised users have strong passwords, and utilising the built-in Unix ipfirewall (or a third party program) allow access to your machine only from trusted IP addresses.

File Transfer Protocol (FTP) is another service requiring serious scrutiny. It allows a degree of access comparable to that a user has when sitting at the keyboard, and also exposes files that are not generally easy to locate or access, even from the keyboard.
Users you allow ftp access too will need UIDs and passwords; anonymous FTP is not supported. Do not allow ftp users Admin priveledges, but general User level. If your system is cracked, and the account that has been compromised to gain access has Admin level priviledges, an intruder is home free once in and can "own" your box.

File Sharing with other Macs is accomplished using the AppleShare authentication protocol, employing Diffie-Hellman Exchange (DHX), providing a secure and easy to use means of information exchange. Regular users will automatically have remote access to there own files within their own home folders. Admin level users have read-only access to all files available on the machine, including those public folders in other users home directories, and guest users are allowed to view files in regular users public folders. Invisible files are not seen by any users.

A "blind" drop box is also accessable to guests who wish to transfer a file to an authorised user. While they can deposit files, they are unable to see that repository's existing contents.

All users can change access priveledges to their own home folders, and Admin users can do so on all files and folders. These permission changes can be done at the command line, but can quickly and easily be done right from the desktop by selecting a folder/file and invoking the Get Info control panel. Guest users are restricted to accessing public folders only.

NOTE: File sharing with MS Windows machines will become available via SMB (Server Message Block) functionality in the first major OSX upgrade, OSX 10.1, to be released in September of 2001.

Web Sharing (http) OSX comes with the Apache web server. Essentially a very secure server package, from the GUI interface, controlling and customising existing security settings can be limiting. For the more Unix-savvy users, CLI-level and config file text editing control is available. Consequently, one must carefully assess the risks at stake in any particular server situation, who is administrating the server and what their skill level is, and take steps accordingly.

When activated, OSX Web Sharing provides access to certain files. Users can create and serve their own web pages from their homepage directories which must be located in their User's home directory at http://<machine IP address>/<~username>. The machine itself has a general "host" website located at http://<machine IP address>/. These files are stored in the /Library/Documents folder inside the webserver folder. These sites are available on the web to admin, non-admin and Guest users equally. Access priviledges cannot be set via the GUI, but users can be assigned to specified groups, and port re-assignments and system logging can be configured from it as well.

Built-in Web Sharing with OSX is fine for LAN or intranet use, but if you'll be serving the WWW on a regular basis, it would be advisable to upgrade to the robust, full enterprise level OSX Server.

NOTE: A more secure version of inetd, xinetd is currently available for OSX. It provides excellent options for securing your server, including interface binding, expansion of logging parameters, and thorough access controls based on source and destination addresses and time stamps. xinetd does have shortcomings where

RPC services are concerned, but both xinetd and inetd can comfortably reside concurrently on the same server.

Firewalls and Access Controls

There are host-based firewalls designed for Mac OS versions prior to OSX, and while they may protect the services running on the 9.x side of the operating system, they will not protect OSX with its FreeBSD/Unix underpinnings and multitude of services. A networked Unix machine must have a firewall!

OSX comes with a built-in firewall, ipfirewall. This is a solid implementation for access control, and can filter packets by type, source/destination address, interface, IP options settings, etc. But once again, it is only configurable from the command line environment.

A third party product, BrickHouse is available as shareware for $25 USD. BrickHouse provides a GUI for configuring many ipfirewall features without accessing the CLI. The interface is not designed for the novice user however. It does not "hand-hold" the user as settings are changed, and much of the dialogue box choices may appear somewhat cryptic.

Symantec has recently released Norton Personal Firewall for OSX. Nearly a twin for its older sibling for "Classic Mac OS", it adresses the issues and vulnerabilities specific to OSX, provides an easy-to-use GUI, and features expanded logging features. While not replacing the embedded ipfirewall, NPF-OSX provides yet an additional, solid layer of network security.

E-mail

Basic e-mail, that is, TEXT ONLY, is quite benign. But the modern world has added many new features to this marvelous utility. Today e-mail can provide previews of a message before opening it (though strictly speaking, if a message is previewed, it's already open). The html version can provide the recipient with text and images and sounds and animations using JAVA, JavaScript, AppleScript, VBS, etc. which, while giving us something nicer to look at or listen to, are far from necessary and have much more important things they should be doing elsewhere. If securing your PC/workstation is a primary objective, then configuring whatever e-mail client you choose should be another step on your checklist.

Most e-mail clients in use today, such as Eudora Mail, Netscape Messenger, or OutLook, install with many potentially risky features turned on by default. Typically, most home users probably enjoy what these features offer. Until they lose the contents of their hard-drive, or contibute to an internet-wide worm or virus infection, at least. Then some of them may rethink their e-mail priorities.

First, if your mail client has a "Preview" mode, turn it off. It does no good to put yourself in the position of bolting the door after the horse has left the barn.

Secondly, keep a close eye on attachments. If they're unexpected, in any way suspicious, or from a questionable source, delete them. Or at the very least, e-mail the sender first to confirm it really came from them, and that they intended to send it! Network worms help themselves to their hosts e-mail address books and happily send themselves on to the next series of unwitting hosts. I limit the size of e-mails I download, so most attached viral files generally exceed my "load limit", so giving me the option of downloading after the fact and generally having foreknowlege of the type of file or it's name.

Third, disable any scripting capabilities your mail client may have, such as Visual Basic Script (VBS) or Javascript. These are not needed to send and receive text-based mail.

Fourth, if your mail client can automatically download images, as in OSX's Mail program, turn this off as well. Again, not needed to send and receive text-based mail. Eudora's client for OSX should also be configured not to run animated GIF files for instance. Any embedded script is a potential security threat.

Simply put, if e-mail content (by that I mean text content) is the main payload of your e-mail activities, stick to text-only. By doing so, malicious code will be unable to execute itself, thereby eliminating such e-

mail-based threats.

Mention should be made of the need to keep certain types of plain-text content confidential. Such content could be of a financial nature, a company's confidential marketing plans, a new automobile design or a proprietary industrial process. The compromise of information in any of these cases could be crippling to a company. Beyond financial loss, current issues of privacy can bankrupt an organisation by its incurring liability responsibility. Protecting this type of data is crucial.

Encryption of data can be accomplished quite easily today with third party software such as PGP (Pretty Good Privacy), which employs PKI (Public Key Infrastructure) technology. Web-based email can take advantage of SSL (Secure Socket Layer), a proprietary technology from Netscape Corp. Explore the options open to you if encryption of mission-critical data is of concern.

For specific e-mail configuration instructions, see the documentation or Help files that accompanied your mail client.

Web Browsers

As web browsers increase in sophistication and functionality, and as more and more commercial transactions are conducted via the WWW, threats of browser-based attacks have increased.

Not only must a web user be concerned that adequate encryption techniques for actual transactions are employed, but must also feel confident that any database-stored customer financial informnation such as credit card numbers is also protected after the transaction is complete.

Much of the e-commerce aspect here is dependent on the security measures taken by the company running the webserver. But within our own browsers today there are steps we can take as well to increase our defensive layers to keep our data confidential, intact, and available when and where needed by those so authorised.

At this time, some of the browsers available for OSX consist of Netscape 6.1, Omniweb, Internet Explorer, and iCab.

Regardless of your choice of browser, steps can be taken to enhance the security level of your browser-based web activities.

In your browser prefernces, disable such features as Active-X controls and Javascript. Many web pages today contain "active content", which as the name implies, can be downloaded along with a web page and its visible contents, (ususally unbeknownst to the user) and affect some change or other to your computer. This is functionally similar to activating a piece of maliciuos code attached to an e-mail message or code embedded in a message and self activated in the usre's Preview pane. These little "applets" quietly go about their business, and if that business is of ill intent, damage will be done before you actually know it.

(There are several third party software packages available to protect some PCs from browser-based attacks. These programs act much like a firewall and can filter out and isolate Java applets, Active-X controls and virii as well.)

Assuring the confidentiality of any transactions also requires some type of encryption methodology. The use of SSL and Digital Certificate technology should be used whenever possible, and is not platform-specific.

Conclusion

The steps outlined above are by no means exhaustive in scope. There are thousands of pages and dozens of books that have been written for the securing of the Unix platform, many specific to FreeBSD, and to cover every aspect of any operating system would be far beyond the limits of such a short paper as this. Two extremely important components of a layered defense initiative for information and network security (appropriate security policy and data and system backup procedures) were not even touched upon. This in no way belittles their importance.

But the seven categories discussd above will at least provide OSX users with a basic foundation on which to build a more extensive layered defense system for their networked or individual PCs. Users should however, keep abreast of OSX and Unix security developemnts, vulnerabilties, and countermeasures in general. There are numerous mailing lists and web sites that provide such information, or links to it. See References and Sources for some suggested resources.

References and Sources

Mac OSX Security

Apple Developer OSX Security - http://developer.apple.com/internet/macosx/securityintro.html

SANS Institute - http://www.sans.org/infosecFAQ/mac/macosx.htm

MacSecurity.Org - http://www.macsecurity.org/

Macintosh Security - http://www.osxsecurity.com/

OSXSecurity - http://www.osxsecurity.com/

OSX Zone - http://www.osxzone.com/

MacWrite.Com - http://www.macwrite.com/macsecurity/

General Internet Security

SANS Institute - http://www.sans.org/newlook/home.htm

http://www.webtechniques.com/archives/2000/06/conn/

Firewalls

http://www.obtuse.com/juniper-docs/ipfirewall/

http://www.symantec.com/consumer_products/sbho-mac.html

World Wide Web Consortium

- http://www.w3.org/Security/

Mailing Lists and Security News sources

Symantec Enterprise Security News - http://enterprisesecurity.symantec.com/content/ESNews.cfm

SANS Internet Storm Center - http://www.incidents.org/

CERT Coordination Center - http://www.cert.org/current/current_activity.html

SecurityFocus Mailing Lists - http://www.securityfocus.com/

Bibliography

Garfinkel, Simson and Spafford, Gene. "Practical UNIX & Internet Security, 2nd Edition" Sebastopol, California; O'Reilly and Associates, Inc.

Stauffer, Todd. "Mastering Mac OSX" Alameda, California; Sybex, Inc., 2001

Lewis, Rita with Fishman, Bill . "Mac OS in a Nutshell " Sebastopol, California; O'Reilly and Associates, Inc., 2001

**Oppenheimer, Alan B., and Whitaker, Charles H. "Internet Security for your Macintosh: A Guide for the Rest of Us"
Berkeley, California; Peachpit Press, 2001**

Zwicky, Elizabeth D. and Cooper, Simon and Chapman, D. Brent. "Building Internet Firewalls, 2nd Edition " Sebastopol, California; O'Reilly and Associates, Inc.

Last Updated: September 19th, 2017

Upcoming Training

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event