Global Information Assurance Certification Paper

Name: Craig Gorme
Version #: 1.3
Title: Mac OS X.1 Security for Home, Office and Internet

Abstract

Apple's OS X brings a new computing paradigm to Macintosh users and administrators. This change offers many benefits, but also presents many challenges; one of these challenges is system security. Out of the box, Apple's new operating system is one of the most secure Unix variants available, but it is not as secure as it must be for a consumer product. Several security features have little or no documentation and some types of security tools are not. This paper examines why OS X is so secure, suggests several third party security to increase system security.

Introduction

Things have changed! Apple's OS X presents new and exciting challenges to Macintosh administrators and home users. Not the least of these challenges is the establishment of a secure computing environment in the home, on the Internet and in the lab. Although there is much that is original in this operating system, a great deal of it has been borrowed from UNIX-like operating systems such as Open Step and FreeBSD (Apple 2, nd). This is of great benefit to us; a bridge has been built from the old to the new. Many of the tools and pitfalls associated with OS X are well documented and an extremely large and talented community is working to find and fix new vulnerabilities before they become well known in the hacker community. This also presents a problem for us; we are in new territory away from the safety of the Macintosh OS we were so used to.

OS X, because of it's Unix underpinnings, is an extraordinary powerful and flexible operating system. The Mac OS is now more stable than it has ever been; it used to be that sometimes only a few hours would go by between crashes, now weeks can go by without having to reboot. The speed of multiple processor systems is now obtainable by Macintosh users; in the past only certain processor intensive programs took advantage of this feature, but now even the operating system's core functions are sped by multiple processors. Not only are our traditional "classic" applications available to us, but also the world of command line applications and powerful open source Unix and Linux software are now at our fingertips (Apple 2, nd).

Unfortunately all this power and functionality comes with a price; traditionally Unix and Unix like operating systems are not very secure (Nemeth, Snyder, Seebass, Hein, 2001 & Ray, Ray, 2001). Unix operating systems were designed with sharing in mind. Serious security was not a priority until November 1988 when after 20 years of Unix use and development the Morris Worm hit the Internet(Nemeth et al. 2001 & SANS, 2001).Even recently Unix operating systems have been hit by buffer overrun exploits like the buffer overflow vulnerability in System V derived logins (CERT/CC, December 2001), viruses and worms like the Sadmind worm (CERT/CC, May 2001)and vulnerable services WU-FTPD (CERT/CC, February 2002). It doesn't have to be this way as OpenBSD shows; it has had no remote holes found in four years (OpenBSD, 2002), and apparently Apple got the message as well.

Security has become one of the biggest concerns to the Unix community and now the Macintosh community as well. In this paper we will be using four key concepts taught by the SANS Institute (Pinkard, 2002 & SANS, 2002) to protect our systems: know your

system; defense in depth; the principle of least privilege; and that prevention is ideal, but detection is a must. Know your system means knowing what applications are running on the computer, what network connections are need to be open and what applications, utilities and file are installed on the system. If something has changed you need to know about it now! Finding out that a Trojan was installed a month ago is not good enough.

Defense in depth is the concept that more than one level of security is needed. Like an onion, which has many layers, your security too should have several layers. This has two effects: (1) if your first layer of defense is compromised there is at another layer to protect your system; and (2) having several layers of defense makes your system unattractive to hackers (SANS, 2002). For example, many users with DSL or Cable connections use Linksys and D-Link routers, in fact if connected to the Internet some sort of router is a must; what if a way is found to defeat the protections these products afford the internal network. Every system on the internal network is now easily compromised; Now what if each internal computer has a software firewall that allows only a small number of network connections. Your systems are still at least somewhat safe especially from script kiddies and at this point they may give up from frustration or lack of skill.

The principle of least privilege is that any users, devices or applications need to be given the least amount of rights they need to do their job (Pinkard, 2002). If a user does not need to install software on OS X do not give them an administrator account. If a device or application does not need complete access to the system then do not give them root access and make new regular accounts for them that have access to only what they need.

The final concept, prevention is ideal, but detection is a must, is a combination of the first three concepts with the added wrinkle of detection (SANS, 2002). It is best from a time, money and a general sense of well being to prevent intruders from compromising your network and systems. If you can't stop a break in you absolutely need to know about it so you can be take care of problem immediately so more data is not compromised.

Backing up these concepts with action is not a guarantee that your network and systems are secure, but it does go a long way towards that goal. Fortunately security was a concern of Apple's when they designed OS X, so things are not nearly as bad as it could be. By thinking about security Apple made it relatively easy to follow the four concepts.

What Apple Did Right

A year with only a couple of minor security advisories is a very good track record for a new operating system; another new operating system had a major security flaw found a month after it was released. Apple did a lot of things right when they put together OS X. First, they disabled many of the non essential services with network ports in the default installation; FTP is off, TFTP is off, finger is off, telnet is off, the web server is off. Each open port is like a door into your computer and keeping a minimum number of ports open minimizes the risk to your system. In fact only four service ports are active (Apple 2, nd): automounter, used for mounting network volumes; syslog, for recording system logs; suprpc, for file sharing and Netinfo, for network authentication and authorization (Stauber, 2001). Having all these non essential services turned off by default is what makes OS X so secure out of the box. Many of these daemons can be turned on in the user interface, with the others you need to get comfortable with the command line interface. Just because you can turn something on does not mean you should. Many of the services mentioned above are off because they are not secure.

It is a good thing that one of the features that Apple did not turn off was the automatic update feature. One of the major problems with most operating systems, or any software for that matter, is keeping up to date with security patches (Apple 1, nd). The name of this service is a little misleading; Apple did not make the whole update process automatic. Only when the system checks for updates is automated. The default is to check for updates weekly. If an update is found the service will notify the administrator and the system will not install any updates without an administrator's approval. I suggest setting this feature to check for updates every day. Remember, you can choose not to install the update, but now you know that one is available for download. It is also suggested by Apple that you keep on top of any updates for open source software you are using (Apple 1, nd).

Root access; in the world of Unix administration and security this can be a scary phrase. Unix operating systems generally have two types of users, normal users who are relatively powerless and the root account which has complete control over the operating system (Apple 2, nd). Apple played around with permissions and added a third type of user, the Administrator. This allowed Apple to secure OS X even more by disabling the root account to protect the system from inexperienced users and malicious attacks. The Administrator account is the first user that is created on OS X. This account is given special privileges such as making new user accounts and installing new software; more functionality than a normal user

and less functionality than the root account. For most tasks these are all the privileges you will ever need, but if it is ever needed, the root account with all it's power and security risks can be enabled.

Apple included a number of security related utilities in OS X. They provided a software firewall, tcp wrappers, ssh and the Network Utility and all of them are installed by default. The firewall called IPFW protects the system from unauthorized network traffic by applying allow and deny rules to traffic to a network interface.

TCP Wrappers serve a similar function to firewalls, they protect the system from unauthorized network traffic, but their method and reach differs. TCP Wrappers offer additional protection, by wrapping small protection applications around your inetd services to monitor, filter and restrict incoming information (Venema, 1997). The some of the inetd services that can be protected this way are: ftp, telnet, tftp, bootp, and imap among others. All of these services are off by default, but if you need them then wrapping them with TCP Wrappers is a great second or third layer of defense. Remember, defense in depth!

SSH is a secure replacement for telnet and it is very useful for making remote connections to your computer or from your computer to other remote systems (OpenSSH, 2002). Remote connections are great for looking at data and running programs that are on machines in another room or even in another city. Traditionally remote connections were made over telnet sessions, but telnet sends passwords and all other data are in clear text over the network and they are also subject to man in the middle attacks. In fact Apple made it easy to turn on SSH in the user interface, but made telnet more difficult to turn on, by requiring the use of the terminal. SSH encrypts all data, including passwords, before sending it over the network where is decrypted by the receiving machine, thus all your data that is going across the network is protected from prying eyes. SSH also offers non-repudiation by using public/private key pairs to ensure the sender's and the recipient's identities. In short, SSH version 2 is a great tool for connecting to remote machines.

Another useful security tool that Apple provides is it's security updates web page at http://www.apple.com/support/security/security_updates.html. This site posts all known OS X vulnerabilities and updates; it should be reviewed often. As of this writing the last update was October 2001, but the next one could come out tomorrow.

Although, as I have pointed out, Apple has done a good job including a lot of security into OS X there are still areas that are lacking. First, there is a lack of documentation and GUI for

configuring and using IPFW and TCP Wrappers. There are no instruction manuals or Apple knowledge base articles about configuring these tools. Second, Apple left several security tool implementations up to third party developers. This includes antiviral software, host based and network based intrusion detection, and log management and analysis.

Configuring OS X for Better Security

IPFW, the firewall that Apple includes with OS X is actually an open source program that was originally included with FreeBSD 2.0 in 1994 (FreeBSD Handbook, 2002). It is what is technically known as a kernel level packet filtering router; meaning that the kernel "compares each packet to a list of rules before deciding if it should be forwarded or not," (FreeBSD Handbook, 2002). If the packet is forwarded it can be used by whatever application it is destined for, but if it is blocked the packet's short life ends. A firewall is usually the first line of defense for a networked computer.

One of the first things to do when preparing to configure the firewall is to find out what ports your computer needs to communicate with other computers. Remember the first principle, know your computer. Do you access the web or run a web server? Then port 80 needs to be open coming into and going out of the computer. Do you use SSH to access remote computers or access your computer from a remote location? Then port 22 needs to be open. Make an inventory of all the network applications that you use and the ports they need open to communicate; also examine the direction of the communication. Some common services and port numbers are: SSH, port 22; ftp, port 23; http, port 80; pop3, port 110; sunrpc, port 111; nntp (news groups), port 119; and ntp (network time), port 123 (IANA, 2002). A list of port numbers and their associated services is located at http://www.iana.org/assignments/port-numbers.

After compiling your list you need to configure the firewall to allow access to all the ports on your list and to deny all the ports that are not on the list. This means creating a catalog of filters for incoming and outgoing network traffic (Arentz, 2000). Currently there are three methods of doing this: first, there are two shareware packages that will help you configure the built in firewall; second, there are several commercial or shareware software firewalls that you can buy; and third, you can configure the firewall manually (VersionTracker, 2002). This report is going to focus on the third choice, but give a little more information on the previous two.

The two packages that will assist in setting up the IPFW are

Brickhouse and sunShield, both are beta software at this time and I have found both to be easy to use, but a little bit rough around the edges. Right now Brickhouse has many more features including a default list of ports to block to protect against various attacks, hacks and trojans. For more information you can visit http://personalpages.tds.net/~brian_hill/brickhouse.html for more information on Brickhouse and http://homepage.mac.com/opalliere/Menu3.html for more information on sunShield.

Four commercial firewalls also exist; these replace the built-in firewall: They are Impasse from http://glu.com/products/impasse/; Firewalk X 2 from http://www.pliris-soft.com/products/firewalkx/index.html; Netbarrier from http://www.intego.com/netbarrier/home.html; and Symantec Norton Personal Firewall from http://www.symantec.com/sabu/nis/npf_mac/index.html. You can visit www.versiontracker.com for reviews and to buy all of these products.

If you want to get comfortable using the terminal or if you already are comfortable you can configure ipfw manually. OS X makes this pretty easy since it is already installed and enabled. For more information on manually building the IPFW rule set see Stephen Arentz's tutorial at http://wopr.norad.org/articles/firewall/.

If you need to enable any of the inetd.conf services then a common and recommended way to protect these services is to enable TCP Wrappers (Gray, 1999 & Ray & Ray, 2001). At this time there are no GUI third party software packages to configure TCP Wrappers so they must be configured through the terminal interface. For a good tutorial on how to configure TCP Wrappers see Ray and Ray, 1999. The basics of configuring TCP Wrappers consists of adding the appropriate filters to two files: /etc/hosts.deny and /etc/hosts.allow (Ray and Ray, 1999).

Apple left out several utilities that third party developers have provided. These are necessary utilities can be broken down into several areas: antiviral, file integrity, intrusion detection, log monitoring and vulnerability analysis. Antivirus is a necessity for all operating systems and OS X is no exception. There are three commercial applications available for OS X, Symantec's Norton AntiVirus 8.0, McAfee's Virex 7.0 and Sophos' Anti-Virus 3.4.8 (VersionTracker, 2002). All are updated regularly, but they all have different features research each product carefully to make sure that it has the features you need and want.

File integrity checking makes a checksum calculation of many important files on your system and then checks those files at a

set schedule to see if the checksum has changed. If a file has changed without your knowledge it may have been replaced by a hacker. With these products it is a good idea to print out a hardcopy of the checksums generated by the product so that if the attacker is able to change the online checksum database you have the hardcopy to further check the database against (SANS, 2002). There are three file integrity options for Mac OS X: Checkmate, md5app and the academic version of Tripwire (Ray & Ray, 2001 & VersionTracker, 2002). The first two have a nice GUI that make installing and using the software very easy, but Checkmate has a built in file list and scheduling features. Tripwire needs to be installed, configured and run using the terminal; for more information see www.tripwire.com and Ray & Ray, 2001.

There are two types of intrusion detection systems (IDS), host based and network based (SANS, 2002) and both types are available for OS X. MacSniffer a utility written by Brian Hill who is also the author of Brickhouse and (Hill, 2002)can be used to log network traffic into and from a OS X system. Also Snort, an open source IDS has been ported to install and run on OS X (Roesch, 2002). Snort is a very powerful and intricate application that was written specifically as a network based IDS. It compares incoming and outgoing network traffic to a database of signatures to see what the traffic actually is doing (Roesch ,2002). Be sure to read the documentation before you install this software, but after you install and use it you will be glad that you did. A Host based IDS application is available from Psionic Software: PortSentry (Psionic, 2002 & Ray & Ray, 2001). They also make another product HostSentry that detects anomalous login issues, but I have not been able to find out if it is OS X compatible (Psionic, 2002). Port Sentry is able to detect, log and respond to port scans and other attacks by using the OS X built in firewall IPFW and TCP Wrappers to block attacking IP addresses (Psionic, 2002). It must be compiled, installed and configured using the command line interface, but there are good installation instructions included with the download; be sure to read them.

Monitoring the log files on OS X is not an intuitive process. You use the Console application that Apple provides to view some logs and others are read by going to /var/log. Also many of the entries can be cryptic in their meaning. Many items in OS X get logged: logins, application crashes, daemons starting and other various messages. Syslog Gen X is a program that provides a GUI to configure the /etc/syslog.conf file to adjust the items that get logged and to move the destination of the log file to a different location; even to a remote computer (The Trafalgar Group, 2002). LogSentry, another application by Psionic

Software, monitors system logs and can email security violations and other events to an administrator (Psionic, 2002). This program also works with there other software and can email an administrator when the system is being probed or attacked (Psionic, 2002). These are two great programs for learning about the log files that OS X generates.

Vulnerability analysis on OS X took a great step forward in ease of use and power when MacAnalysis was released. This is an easy to use and powerful program that let you scan Macintosh as well as Unix and Windows machines for many vulnerabilities including CGI problems in web servers, open shares, open ports, OS fingerprinting and installed Trojan detection (MacAnalysis, 2002). Newer versions also includes a built in firewall that is still in beta testing. Other GUI tools are included to scan networks, trace IP addresses and check mail server vulnerabilities. After a scan is complete the software can issue a report about what vulnerabilities were found. This application is great for finding out more about your system and network, but get permission before using it on machines other than your own (SANS, 2002).

Apple appears to have worked very hard to make Macintosh OS X a secure operating system, and their efforts paid off. Out of the box OS X is very secure and when security issues have been found they have been taken care of quickly through the automatic update feature. Even with this security mind set, Apple left several important tools to third party developers and consumers and administrators need to know about these tools to adequately protect their systems. Using many of the tools and applications mentioned in this report will not guarantee security, but it can give you piece of mind that it will be difficult to break into your system and if someone does than you will be notified. Other areas that need to be examined are securing single user sign on, booting from other devices, and protecting Netinfo passwords.

References

Apple Computer 1, (nd). Security: Mac OS X and Unix. Retrieved February 12, 2002, from http://developer.apple.com/internet/maxosx/securitycompare.html

Apple Computer 2, (nd). An Introduction to Mac OS X Security. Retrieved February 12, 2002, from http://developer.apple.com/internet/macosx/securityintro.html

Arentz, S., (2000). Building your own personal firewall. Retrieved March 2, 2002 from http://wopr.norad.org/articles/firewall/

CERT® Coordination Center, CERT/CC Advisories (2001, December 18). CERT® Advisory CA-2001-34 Buffer Overflow in System V Derived Login. Retrieved February 26, 2002, from http://www.cert.org/advisories/CA-2001-34.html

CERT® Coordination Center, CERT/CC Advisories (2001, May 10). CERT® Advisory CA-2001-11 sadmind/IIS Worm. Retrieved February 26, 2002, from http://www.cert.org/advisories/CA-2001-11.html

CERT® Coordination Center, CERT/CC Advisories (2002, February 15). CERT® Advisory CA-2001-33 Multiple Vulnerabilities in WU-FTPD. Retrieved February 26, 2002, from http://www.cert.org/advisories/CA-2001-33.html

CERT® Coordination Center, CERT/CC Advisories

FreeBSD Documentation Project, (2002). FreeBSD Handbook. Retrieved February 12, 2002 from http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/security.html

Gray, Bob, (1999, June). Security on a Source Code Unix System. Retrieved February 12 ,2002 from http://www.usenix.org/publications/login/1999-6/features/sourcecode.html

IANA, (2002). Port Numbers. Retrieved February 26, 2002 from http://www.iana.org/assignments/port-numbers

Hill, Brian, (2002), Home Page. Retrieved February 26, 2002 from http://personalpages.tds.net/~brian_hill/

MacAnalysis (2002). MacAnalsys Home Page. Retrieved February 12, from http://www.macanalysis.com/about.php3

Nemeth, E., Snyder, G., Seebass, S., Hein, T.R. (2001), Unix System Administration Handbook, (3RD Ed.). New Jersey: Prentice Hall PTR.

OpenBSD, (2002, January 29). Home Page. Retrieved February 26, 2002, from http://www.openbsd.org

OpenSSH, (2002, February 12). Home Page. Retrieved February 26, 2002, from http://www.openssh.com/

Pinkard, Becky. (2002, January). Security Essentials: Network Fundamentals. Presentation at SANS South Beach, Coral Gables, FL.

Psionic Software, (2002). Home Page. Retrieved March 3, 2002 from http://www.psionic.com/

Ray, J., Ray, W.C., (2001) Mac OS X Unleashed, New York: SAMS Publishing

Roesch, Marty 1, (2002). Snort Home Page. Retrieved February, 12, 2002 from http://www.snort.org

Roesch, Marty 2, (2002). Snort FAQ. Retrieved February, 12, 2002 from http://www.snort.org/docs/faq.html

SANS Organization. (2002). SANS South Beach Conference: Security Essentials.

Stauber, L., (2001). Mac OS X: A Brief Introduction. Retrieved February 26, 2002 from http://www.occam.com/leonvs/computer/osx/intro/05.html

Trafalgar Group, (2002). Syslog Gen X Home Page. Retrieved March 2, 2002 from http://www.thetrafalgargroup.net/sysloggenx

Venema, Wietsel, (1997). TCP Wrappers Blub file. Retrieved February 12, 2002 from ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB

Version Tracker-Mac OS X, (2002). www.versiontracker.com. Retrieved March 2, 2002 from http://www.versiontracker.com/mp/new_search.m?productDB=mac&mode=Quick&OS_Filter=MacOSX&search=firewall

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor