MacOS X: Is Apple opening Pandora's Box?

Thomas Crow
December 4, 2000

With both positive and negative fanfare, Apple Computer released a Public Beta of its next generation operating system in the Fall of 2000. The purpose of this paper is to explore briefly some of the security implications that this new operating system brings to play by first looking at what composes the new operating system and then touching on areas of concern typical for most operating systems.

MacOS X Heritage

MacOS X is a radical change from the current "classic" MacOS, now in revision 9.04. Apple has leveraged the Mach 3.0 kernel and the BSD 4.3 Operating System to offer a true multi-user and multi-tasking operating environment. Apple is currently using FreeBSD as its reference platform for compatibility with BSD. The unique pairing of the Mach kernel and the BSD OS, which form the core of the new operating system, are the results of an ongoing open source effort referred to as Darwin. Given that Apple is best known for its user interface and that FreeBSD is the muscle behind major websites like Yahoo, the potential is there for an operating system that could be a web server, a software development platform, or a home computer and do each equally well.

Services

One of the primary means for an attacker to compromise a system is through the services that it provides. Even if access to such services could be restricted, sometimes there can be a flaw in the implementation that could provide a way to circumvent the restriction. Traditionally, the Macintosh platform hasn't had much in the way of services to provide to the Internet at large. In addition to continuing support for AppleShare over IP, MacOS X can potentially provide many more services that a hacker could compromise. While familiar to those in the UNIX community, these new services, like telnet and ftp, might be unfamiliar to many Macintosh users. An examination of the BSD UNIX layer via the Terminal Shell application reveals a default install that follows security best practices. All services controlled by the inetd daemon are disabled by default. Appleshare is disabled by default. The number of ports actively listening is also quite limited. From the outside there isn't much to see, a TCP scan of a MacOS X system using the vulnerability scanner nmap does not yield much in the way of information. All in all, this is not a bad state for a freshly installed operating system to be in.

Viruses and Malware

Protection from viruses and malware still hinges user behavior and the configuration of the system. The BSD filesystem protections will limit the scope of a virus, worm, Trojan horse, or other types of malware to the permissions that the user has.   Like Windows NT, there is a temptation to make the normal user account the administrator account to save a little time. Unfortunately, doing so will give the malware the opportunity to operate as the administrator of the system. For that reason, there will still be a place for Anti-Virus programs under MacOS X. At this time, none of the major anti-virus software developers have released versions for MacOS X. It will also be a good practice to not create every-day user accounts with administrator privileges. Many common adminstrative functions can be accessed from the System Preferences Application. This application will prompt for the root password when needed. Until anti-virus programs appear, good protection from malware will have to come from security conscious users and administrators.

Firewalls and Intrusion Detection

An examination of the configuration file for the inetd daemon reveals that tcp wrappers are installed by default with a standard install. However, the hosts.allow and hosts.deny files are not configured. Given access to a command line and the root password, that situation can easily be corrected.

MacOS X comes equipped with the IPFW firewall software already installed. Using tutorials already available on the World Wide Web, one can configure this rule-based firewall system to better protect your system from unwanted attention. This is particularly important if the system is always connected to the Internet either via a leased-line or a broadband (cable modem or DSL) connection. If the user is not comfortable with the command line interface, there now exists GUI-based software packages to configure the firewall. An excellent example is the *Brickhouse* program.

In the arena of Intrusion detection, the BSD logfiles are viewable from command line. Although I haven't encountered a port to MacOS X yet, an administrator with access to a compiler should be able to make use of any of the current freeware logfile analyzers or configure syslog to send data to a central logger. In addition, the GNU Perl scripting language is part of the standard software load. The addition of system logging to MacOS is a welcome one for security conscious administrators.

Encryption

Like many of the BSD variants, MacOS X Public Beta includes the OpenSSH client and server software. This enables the user to perform encrypted communications with other systems. The ssh command invokes a secure remote shell similar to the rsh utility commonly found on UNIX and UNIX-like operating systems. Similarly, the scp command performs the same function as the rcp utility. By default the server software is not started on the MacOS X Public Beta.

According to several sources, Apple has been working with MIT to produce a version of the Kerberos authentication system for the final MacOS X release. A version of PGP or GnuPGP would be another welcome addition.

Denial of Service

Defense against denial of service attacks is a primary concern for administrators of any computing platform on the Internet. The BSD network stack has been refined and tested over the years. Also, the Open Source nature of Darwin lends itself to faster detection and correction of defects. In theory, the new operating system should be less susceptible to DOS attacks than the current MacOS.

Users

MacOS 9 introduced to Macintosh users the concepts of multiple users and administrative users; however, this concept is optional. Under MacOS X, this concept is the normal way of doing business. Another welcome change is due to the permission scheme inherited from BSD. The classic MacOS did not have the concept of ownership; hence, any user of the system could see the other users' files. UNIX on the other hand breaks down file permissions by owner, group, and the world.

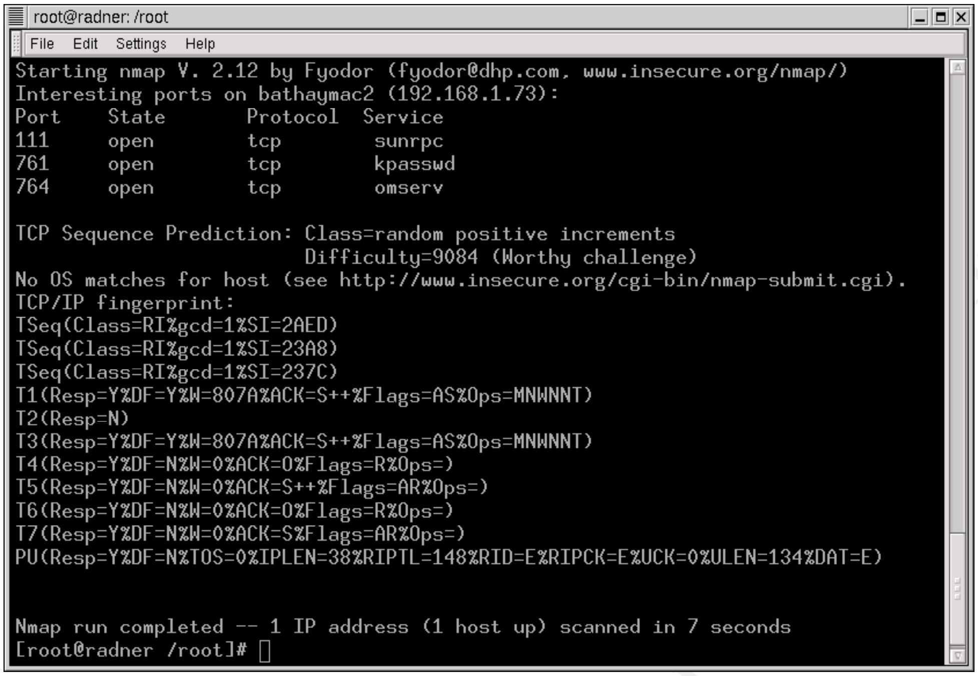
Although no official word has come from Apple, it is likely that the Terminal application and some of the underlying BSD UNIX environment will be inaccessible in the final release. This has often been called a security feature of the classic MacOS, although some refer to it as an accidental feature. Many in the developer community hope that the Terminal will be available as an add-on for "power users."

Conclusion

The real question to be posed is how much of the Public Beta functionality will be present in the final release and what additional features will appear. If the Public Beta reflects the security posture of the final release, Pandora's Box will be kept closed.

Appendix A

Output of nmap on a freshly installed MacOS X Public Beta System



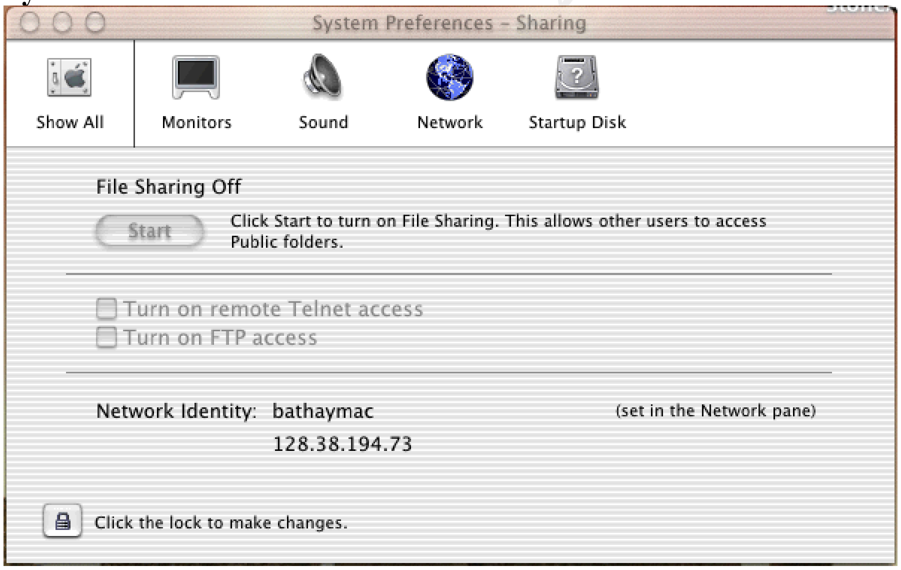
```
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on bathaymac2 (192.168.1.73):
Port    State       Protocol  Service
111     open        tcp        sunrpc
761     open        tcp        kpasswd
764     open        tcp        omserv

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=9084 (Worthy challenge)
No OS matches for host (see http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
TSeq(Class=RI%gcd=1%SI=2AED)
TSeq(Class=RI%gcd=1%SI=23A8)
TSeq(Class=RI%gcd=1%SI=237C)
T1(Resp=Y%DF=Y%W=807A%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=807A%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=0%ULEN=134%DAT=E)


Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
[root@radner /root]# 
```

Appendix B

System Preferences - Shares Control Panel



File Sharing Off

Click Start to turn on File Sharing. This allows other users to access Public folders.

□ Turn on remote Telnet access

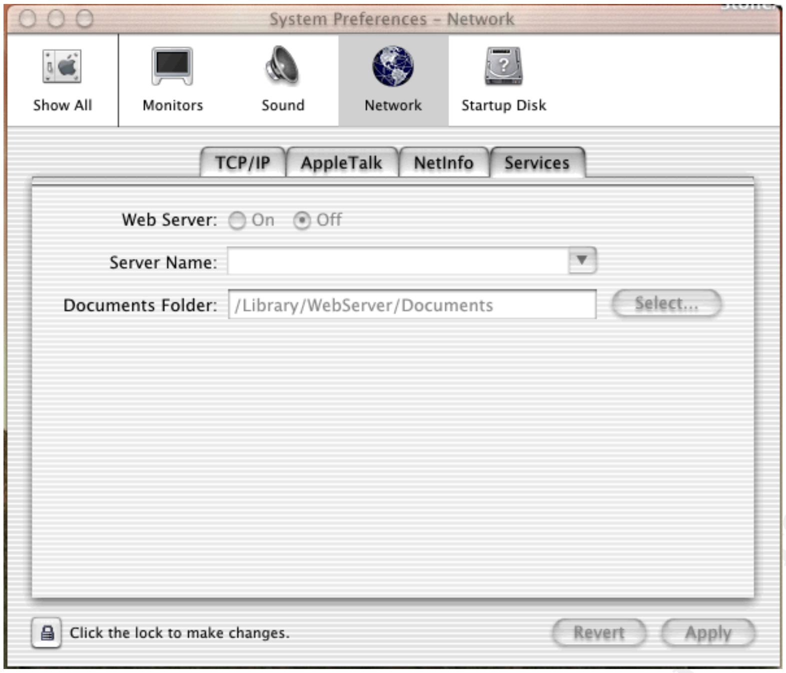
□ Turn on FTP access

Network Identity: bathaymac (set in the Network pane)
128.38.194.73

Click the lock to make changes.

Appendix C

System Preferences – Network – Services Control Panel



Web Server: ○ On ● Off

Server Name:

Documents Folder: /Library/WebServer/Documents

References

"Darwin: Frequently Asked Questions." URL: http://www.publicsource.apple.com/projects/darwin/faq.html

"MacOS X Public Beta Forums." URL: http://www.macosx.com/

"MacOS X Information Archive" 13 January 2000. URL: http://www.appleinsider.com/macosx.shtml

Sellers, Dennis. "Road to MacOS X: Security and OS X" 23 June, 2000. URL: http://www.maccentral.com/2000/06/23/

mrpetey@securemac.com. "OS X Security." URL: http://www.securemac.com/osxsecurity.cfm

Hubbard, Jordan. "Open-sourcing the Apple." URL: http://www.salon.com/tech/review/2000/11/17/hubbard-osx/index.html

Arentz, Stefan. "Building your own personal firewall" 9 October, 2000. URL: http://wopr.norad.org/articles/firewall/

Harris, Patrick. "Macintosh Internet Security Basics" 15 September, 2000. URL: http://www.sans.org/infosecFAQ/mac_sec.htm.

Hill, Brian. "Brickhouse." URL: http://personalpages.tds.net/~brian_hill/brickhouse.html

Welch, John C. “The Network Manager: MacOS X On The Network” 23 June, 2000.
URL: http://www.creativepro.com/story/new/0,1819,6612,00.html