Global Information Assurance Certification Paper

Macintosh Internet Security Basics
Patrick Harris

Many of us own or manage Apple Macintosh computers and may wonder how big an issue security is for Macs. What measures should Mac users take to provide for a more secure computer? Are Macintosh computers susceptible to the usual threat vectors? The bad news is, Macs are just as vulnerable to security risks as other Internet-connected computer systems. The good news is that it is possible to combat the security risks with tools provided by Apple and third-party vendors.

Apple historically provided services through their own proprietary networking scheme, AppleTalk. Starting with Mac OS 9 and AppleShare IP, Apple has migrated their services to run over TCP/IP. You can still access services through traditional AppleTalk but since it is not possible to route AppleTalk directly over the Internet, I will focus on securing those services that can be accessed through TCP/IP.

There are security issues that Macs have in common with other platforms and some that are specific to the Mac platform. Macintosh computers were vulnerable to the "Ping of Death," as were other platforms.[1] Microsoft Word macro viruses can infect Mac or PC documents and can spread between the two platforms. There are relatively few known exploits that target the Macintosh specifically. The small number of Macintosh specific exploits and viruses are probably due greatly to the smaller percentage of Macintosh computers on the Internet compared to other operating systems such as Windows and Linux. This may make the Macintosh a less lucrative target for the creators of viruses and exploits. However, this should not lead to a false sense of security.

In late 1999 a university researcher discovered a possible Denial of Service (DOS) attack, which might have leveraged Mac OS 9 computers as pawns in an attack.[2] John Copeland, of Georgia Tech, noticed some unusual packets while doing Internet research, which were apparently targeted at Macs running OS 9. After further study, it was determined that these packets could be used in a Denial of Service attack using Macs as the intermediary. Thankfully, it was caught before it had been used in an actual DOS. Apple has released an update[3] that fixes this and other security issues.

Changes with Mac OS 9

If you wish to use Macintosh File Sharing and Program Linking over TCP/IP, the services that traditionally ran over AppleTalk, or Web Sharing, it is important to understand the security architecture built into the operating system. Program Linking is the mechanism that programs use to communicate with each other such as Apple Events and AppleScript. The Users & Groups tab of the File Sharing control panel is used to control access to these services. By setting up user/group accounts and passwords it is possible to control who has access to each service you are running. By using the built-in Guest account you can grant access without using a password. Use caution when specifying Guest access. Unless you want to have files publicly

accessible then it would be wise to disable Guest access. The exception to this rule is if you want to run a personal web server that would be accessible by the public.

When setting up areas on your computer for access, whether for file sharing or web, it is advisable to limit access by setting up directories for sharing as opposed to sharing your whole hard drive. A good rule to keep in mind is to only allow enough privileges and scope for the user to access the resources they need.

Viruses and Other Malicious Software

Hopefully, everybody is aware of the threat that is posed by viruses, trojans and worms. Although the Mac is not at risk from the latest Visual Basic script worms such as VBS.LoveLetter.A or it's variants, these demonstrate the destructive potential of such mechanisms. Macs could be at risk if someone created a worm that used the AppleScript scripting language found on most Macintosh computers.

The last big threat to the Macintosh community from malicious software was the AutoStart worm, a.k.a. the Hong Kong virus, which spread rapidly through PowerPC-based Macintosh computers worldwide.[4] This worm takes advantage of a feature in QuickTime 2.0 or greater that allows a program or document to be opened when a drive is mounted. You can disable this feature in QuickTime 2.5 or greater by deselecting the CD-ROM AutoPlay feature in the QuickTime control panel.

There are a number of good anti-virus packages available for the Macintosh including Norton AntiVirus (NAV), Intego VirusBarrier, Dr. Solomon's Virex and Sophos Anti-Virus. The most important thing to remember with any anti-virus software is that it is only as good as it's most recently installed virus definitions. Some of the anti-virus products have the ability to automatically update their definitions (NAV, VirusBarrier) while the others require a manual download and installation. The choice of which product to use is best left up to you to decide which best fits your organization or individual use.

Firewalls/NAT

Firewalls and/or proxy servers already protect many multi-platform corporate and business networks connected to the Internet. Administrators should take into account network activity associated with common Macintosh services when building their rulesets. Port numbers associated with these services are listed in Appendix A. Home users and Macintosh-only businesses should consider implementing firewalls at the network and/or desktop level. Even though there are relatively few choices in the Macintosh marketplace filling this niche, it is still possible to find a product that fits your needs and budget.

OpenDoor's DoorStop Personal Firewall is an inexpensive product that offers a user simple protection for their desktop. It offers easy configuration for the three services that can be run on a Mac workstation, Web Sharing, File Sharing over TCP/IP, and Program Linking over TCP/IP

and a blanket filter for all other services. In advanced mode, DoorStop Personal Firewall permits creation of more extensive filters. OpenDoor's Server edition offers a similar interface but greater flexibility in creating filters for Internet traffic.

Intego's NetBarrier includes highly configurable firewall protection as well as a number of other protection and monitoring capabilities. NetBarrier includes protection against DOS attacks, port scans, intrusion attempts in addition to adding TCP sequence number scrambling, monitoring and logging of AppleTalk and TCP/IP traffic and filtering of outgoing traffic.

If you are connecting a network to the Internet, Network Address Translation (NAT) products such as one of Vicomsoft's line of products or Sustainable Networks IPNetRouter should fit your bill. NAT technology provides built-in firewall protection since it effectively hides your network behind your public IP address and only allows connections originating from your internal network.[5] Many NAT products allow limited access to your internal network by using port mapping. Port mapping allows requests for particular services, such as web server access on port 80, to be redirected to a computer on your internal network running that service.

Encryption

With Mac OS 9 Apple has introduced the ability to encrypt, decrypt and verify files with the addition of Apple File Security and Apple Verifier tools. Apple File Security allows you to encrypt your files with a 56-bit symmetric key. You can share your encrypted files with other Mac OS 9 users as long as they have been given the passphrase used when encrypting the file. Apple Verifier is used for verification of digital signatures used to 'sign' files to guarantee authenticity of the sender.

If you wish to share files with people on other platforms, need to use stronger encryption, looking for integration into email programs or need Virtual Private Networking (VPN), PGP (Pretty Good Privacy) is a better alternative. PGP is a public key cryptosystem that offers a choice of different encryption technologies and key lengths depending on security needs. PGP is available either as freeware for personal, non-commercial use from MIT or as a commercial package available from PGP Security.

Final Words

With the increasing availability of high-speed full-time Internet connections, security is an ever-growing concern for all computer users. As many crackers have taken to refining their skills on the relatively undefended home computer users with full-time connections, it is important that home users take precautions to harden their systems as would business users. Armed with an increased awareness of computer security issues and tools it is possible to create a safe and secure computing environment.

Appendix A

Port Numbers Commonly In Use On Macintosh Computers/AppleShare IP

Port	Service
20	FTP data
21	FTP control
25	SMTP
53	DNS
80	HTTP
106	PASS (change password)
110	POP3
119	NNTP
123	NTP
139	NETBIOS Session
143	IMAP
311	AppleShare IP Remote Admin
384	ARNS (tunneling)
387	AURP (tunneling)
497	Retrospect
510	FirstClass server
515	LPR
548	AFP (AppleShare)
591	FileMaker Pro Web
626	IMAP Admin
660	Mac OS Server Admin
687	Shared Users & Groups
1443	WebSTAR/SSL Admin
3031	Program Linking (Apple Events)
4199	EIMS Admin
5003	FileMaker Pro

Appendix B

Online Information Resources

Security Sites

SecureMac – http://www.securemac.com
SANS Institute – http://www.sans.org
CERT Coordination Center – http://www.cert.org
Exploit World: Mac Section - http://www.insecure.org/sploits_mac.html

Antivirus software

Dr. Solomon's Virex - http://www.drsolomons.com/
Intego VirusBarrier – http://www.intego.com/virusbarrier
Norton Antivirus - http://www.symantec.com/nav/nav_mac/
Sophos Anti-Virus - http://www.sophos.com/products/antivirus/savmac.html

Firewall/NAT software

Intego NetBarrier - http://www.intego.com/netbarrier
Open Door Networks – http://www.opendoor.com
Sust. Networks IPNetRouter -
http://www.sustworks.com/site/prod_iprouter_overview.html
Vicomsoft – http://www.vicomsoft.com/

Encryption

PGP Freeware - http://web.mit.edu/network/pgp.html
PGP Commercial - http://www.pgp.com

---

[1] Ford, Ric. "Macs and the 'Ping of Death'." URL: http://www.macintouch.com/pod.html
[2] Copeland, John. "The "Mac DoS Attack," a Scheme for Blocking Internet Connections." 22 December 1999. URL: http://people.atl.mediaone.net/jacopeland/macattack.html
[3] "Open Transport 2.6: Differences Between Open 2.5.x." 3 April 2000. URL: http://til.info.apple.com/techinfo.nsf/artnum/n32075
[4] Ford, Ric. "The AutoStart Worm: a rampant, worldwide threat to Power Macintosh systems." URL: http://www.macintouch.com/hkvirus.html
[5] Tubbs, Guy. "Network Address Translation." 12 November 1999. URL: http://www.vicomsoft.com/knowledge/reference/nat.html

Last Updated: July 23rd, 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